

Subject Index

A

- ACCEPTING A SOC 2® EXAMINATION ENGAGEMENT** 2.01–90
- Agreeing on terms of engagement 2.32, 2.70–90
 - Changes in terms of examination 2.75–78
 - Competence of engagement team members 2.39–42
 - Engagement acceptance and continuance 2.31–34
 - Independence of service auditor 2.05, 2.35–38
 - Management of service organization's responsibilities 2.03–29
 - Preconditions of SOC 2® engagement 2.43–65
 - Service auditor's responsibilities ... 2.30, 2.74
 - Written assertion and representations request of service organization management 2.66–69
- ADDITIONAL SUBJECT MATTERS AND CRITERIA, ADDRESSING IN SOC 2® EXAMINATION** 1.50–54, Table 1-3 at 1.50
- ADVERSE OPINION** 3.29, 4.14, 4.54–55
- ALERT PARAGRAPH, SERVICE AUDITOR'S REPORT** 4.34, Table 4-3 at 4.32
- ANALYTICS** 3.117, 3.143
- APPLICABLE TRUST SERVICES CRITERIA.**
See also trust services criteria 1.05, 1.16, 1.32, 3.92–94, 4.77, Table 1-2 at 1.41, Table 4-4 at 4.116, Supplement B
- ASSURANCE SERVICES EXECUTIVE COMMITTEE (ASEC)** 1.29, 1.36, 2.57
- AUDIT EVIDENCE**
- Evaluating 3.182–189
 - Concluding on sufficiency and appropriateness of 4.05–09
- AUDIT OPINION.** *See opinion*
- AUDIT SAMPLING, TESTS OF CONTROLS** 3.142–146, 3.173, 4.19
- AUTOMATED CONTROLS, TESTS OF** ... 3.138
- AVAILABILITY**
- Applicable trust services criteria Table 1-2 at 1.41, Supplement B
 - Boundaries of the system and 1.22
 - Defined 1.37
 - In description of the system 3.26, 3.34
 - Service organization controls relevant to 1.04, 3.149

B

- BOUNDARIES OF SERVICE ORGANIZATION'S SYSTEM**
- Areas covered by 1.21–23
 - Distinguishing between SOC 1®, SOC 2®, and SOC 3® engagements and related reports 2.45, Appendix B
 - Identifying controls outside of 3.32
 - Management's assertion in SOC 3® report 2.167, 4.112–114
 - Planning the examination 2.75, 2.113
- BUSINESS PARTNERS**
- Prospective 1.10
 - Relationship to service organizations 1.01–04
 - Risk consideration 3.147–151
 - As specified parties of a SOC 2® report 1.09

C

- CARVE-OUT METHOD**
- CCOs. *See complementary subservice organization controls*
 - Defined 2.12
 - Description of the system, contents of ... 3.42
 - Disclosures related to subservice organizations 3.46–54
 - Management responsibilities for use of 2.12–16
 - Materiality related to 3.77
 - Service auditor's report 4.32, 4.39–41, Appendix D-1
 - Suitability of design of controls, evaluating 3.86, 3.99–100, 3.152
- CHANGES TO CONTROLS**
- Evaluating and testing 2.58, 3.140–141
 - Omission from description of the system 4.72
- CHANGES TO THE SYSTEM**
- Omission of relevant changes in description 4.72
 - During the period 3.55–56, 3.62, 3.108, 3.140–141
 - Between periods 3.57–58
- COMMITMENTS TO USER ENTITIES.** *See service commitments and system requirements*
- COMMON CRITERIA.** *See also trust services criteria* 1.39–43, Table 1-2 at 1.41
- COMPETENCE**
- Engagement Team Members 2.39–42
 - Internal audit function 2.132, 2.139–144, 2.146, 3.166

COMPETENCE—continued

- Other practitioner 2.156
- Performance of controls 3.79, 3.98, 3.102, 3.106
- Specialists 2.160-161, 3.178
- Written representations 3.209, 3.222

COMPLEMENTARY SUBSERVICE**ORGANIZATION CONTROLS (CSOCs)**

- Disclosures related to carve-out subservice organizations 3.46-54
- Identification of 2.17-19
- Omission from description of the system, illustrative separate paragraphs 4.74
- In separate SOC 2[®] report analysis 2.114
- Service auditor's report 4.32, 4.39-41, Table 4-3 at 4.32, Appendix D
- Tests of controls 3.152-155

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

- Disclosure of 3.36-41, 3.88-91
- Identification of 2.20-25
- Omitted from description of the system, illustrative separate paragraph 4.73
- In a separate SOC 2[®] report analysis ... 2.114
- Service auditor's report 4.32, 4.36-38, Appendix D, Table 4-3 at 4.32
- SOC 3[®] engagement 2.171
- Suitability of design of controls, evaluating 3.86,

CONFIDENTIALITY

- Applicable trust services criteria Table 1-2 at 1.41, Supplement B
- Boundaries of the system and 1.23
- Defined 1.37
- Privacy distinguished from 1.25-26
- Service organization controls relevant to 1.04

CONTROLS. See also trust services categories; trust services criteria

- Changes to, evaluating and testing 2.58, 3.140-141
- Comparing description to implementation 3.22-23
- Controls that did not operate during the period 3.156
- CSOCs. See complementary subservice organization controls
- CUECs. See complementary user entity controls
- Deficiencies in. See deficiencies in controls
- In description of service organization's system 3.30-32, 3.163, Table 3-1 at 3.30
- Design of. See suitability of design of controls
- Effectiveness of. See operating effectiveness of controls
- Consideration of entity-level controls in planning the examination 2.127-131
- System description, evaluating 3.12-23
- Management's responsibility for ... 2.04, 2.26

CONTROLS—continued

- Not implemented but included in description, illustrative separate paragraph 4.70
- Not operating during the period 4.86-88
- Omission of relevant changes in description of the system 4.72
- Operating effectiveness of. See operating effectiveness of controls
- Planning the examination 2.110, 2.113
- Risk assessment 2.125-126
- Service auditor's recommendations for improving 4.94
- Subservice organizations 2.06-10, 3.43-54
- Suitability of design. See suitability of design of controls
- Tests of. See tests of controls
- User entities reviewing 1.04

CRITERIA. See description criteria; trust services criteria**CSOCs. See complementary subservice organization controls****CUECs. See complementary user entity controls****CYBERSECURITY RISK MANAGEMENT EXAMINATION AND REPORT 1.63-68, Appendix C****D****DATA**

- Reliability of, in tests of controls 3.121-130
- As system component 1.20

DATE OF SERVICE AUDITOR'S REPORT. See also periods Table 4-3 at 4.32, Table 4-4 at 4.116**DEFICIENCIES IN CONTROLS. See also deviations**

- Communicating incidents of 3.193-196
- Defined 3.10, 3.101-102
- Effect on third parties 3.163
- Entity-level controls 2.129-130
- Evaluating results of procedures 3.185
- Forming the opinion 4.10-12
- Identifying and evaluating 3.70-71
- Modifications to management assertions due to 3.228, 4.38
- Occurring during the original, extended, or modified period 2.87-90, 3.132-133
- Operating effectiveness of controls 4.85
- Suitability of design of controls 3.101-105, 4.79-82
- Testing for 3.185-189

DEFINITIONS Appendix I

DESCRIPTION CRITERIA **Supplement A**

- Assessing suitability of 2.57–58
- Disclosures about service commitments and system requirements 3.24–3.26
- System incidents 3.33–35
- User entity responsibilities and CUECs 3.36–41, 4.37
- Disclosures related to subservice organization 3.38, 3.42, 3.47
- Significant changes to service organization's system 3.55–58, 3.108
- Description's requirements for meeting 3.17–19
- Evaluating against description of the system 3.20–23
- Generally 1.05, 1.15–17, 1.27–30
- Materiality considerations 3.72–78
- Misstated or misleading information 3.67
- In SOC 2® report Table 1-1 at 1.18

DESCRIPTION OF SERVICE ORGANIZATION'S SYSTEM

- Boundaries. See boundaries of the system
- Qualitative factors 3.163
- Changes to the system occurring between periods covered by type 2 exam ... 3.57–58
- Confidentiality or privacy principle in 3.59
- Controls. See controls
- Criteria for evaluating. See description criteria
- CUECs and user entity responsibilities 3.36–41
- Entity-level controls disclosures in 2.131
- Evaluating results of procedures 3.183–189
- Generally 1.07, 3.12–23
- Information not covered by the service auditor's report 4.95–104
- Management's responsibility for ... 1.16, 2.26, 2.117
- Materiality consideration. See also material misstatement, risk of 3.07, 3.72–78
- Misstated or misleading description, considering 3.64–68
- Misstatements, identifying and evaluating 3.10, 3.69–71
- Performing a SOC 2® examination ... 3.12–78
- Planning the examination 2.113, 2.116–117
- Procedures to obtain evidence about 3.59–63
- Service commitments and system requirements 2.59–65, 3.24–29
- Significant changes to the system during period covered by type 2 exam ... 3.55–56, 3.62, 3.108
- Subsequent event effects 3.214–219
- Subservice organization considerations 2.11–16, 2.24–25, 3.42–54, 4.75
- System incident disclosures 3.33–35
- Uncorrected misstatements and deficiencies 4.10–12

DESIGN OF CONTROLS. See *suitability of design of controls*

DEVIATIONS

- Changes in terms of engagement 2.76
- Defined 3.10
- Discovery of uncorrected errors 3.193, 3.203
- Effect on suitability of design of controls 3.163
- Evaluating results of procedures 3.185
- Identifying and evaluating 3.157–3.160
- Materiality concept in disclosing 4.16
- As result of intentional acts 3.163, 3.190
- Reporting 4.15–22, Table 4-1 at 4.15

DISCLAIMER OF OPINION

- Change in terms of examination 2.78
- Independence of service auditor and 2.38
- For other information service organization appends to report 4.104
- Service auditor's report 4.61–67, Appendix D-3
- Written representation issues 3.211, 4.66–4.67

DOCUMENTATION. See *also service auditor's report; written assertions; written representations*

- Management's risk assessment 2.55, 2.119, 3.97
- Performing a SOC 2® examination 3.221–225

E

EFFECTIVENESS OF CONTROLS. See *operating effectiveness of controls; suitability of design of controls*

EMPHASIS-OF-MATTER PARAGRAPHS, IN SERVICE AUDITOR'S REPORT 4.89–90

ENGAGEMENT LETTER 2.27, 2.70, 2.74

ENGAGING PARTY

- Signing of engagement letter 2.74
- Written representation when not responsible party 3.212

ENTERPRISE IT OUTSOURCING SERVICES, DEFINED 1.02

EVIDENCE. See *audit evidence*

EXPECTED KNOWLEDGE OF SPECIFIED PARTIES 1.08–13

EXTENDING OR MODIFYING THE PERIOD COVERED BY THE EXAMINATION 2.79–90

F

FINANCIAL TECHNOLOGY (FINTECH) SERVICES 1.02

FRAUD CONSIDERATION

- Operating effectiveness of controls evaluation 3.162
- Planning the examination 2.122
- Responding to and communicating known or suspected fraud 3.190–196
- Suitability of design of controls evaluation 3.86, 3.162
- Written representations about fraud 3.203

H**HEALTH CARE CLAIMS MANAGEMENT AND PROCESSING, DEFINED 1.02****I****INCLUSIVE METHOD**

- Defined 2.12
- Description of the system, contents of 3.43–45
- Design of controls for subservice organization, evaluating 3.81
- Illustrative service auditor's report Appendix D-2
- Management responsibilities in deciding on 2.12–16
- Operating effectiveness of controls for subservice organization, evaluating 3.81
- Planning considerations for using 2.96–103
- Subservice organization's management responsibilities 2.28

INDEPENDENCE OF SERVICE AUDITORS

- Accepting a SOC 2[®] examination engagement 2.05, 2.35–38
- Other practitioner consideration 2.156
- Specialist, use of 2.162–163
- Subservice organizations consideration 2.15, 2.37

INFRASTRUCTURE, DEFINED 1.20**INHERENT RISK, DEFINED 2.124****INTENDED USERS. See also user entities**

- Business partners 1.01–.04, 1.09, 1.10,
- Description criteria as based on informational needs of 3.67
- In engagement acceptance and continuance 2.47–48
- Expected knowledge of 1.08–13
- Auditor report considerations 1.07–13
- Need for subservice organization information 3.48
- Service auditor's evaluation of design of controls to serve 3.163

INTERNAL AUDIT FUNCTION, USING WORK OF 3.166–177

- Direct assistance from 3.176–177, 4.24–26
- Evaluating adequacy of work of ... 3.170–174

INTERNAL AUDIT FUNCTION, USING WORK OF—continued

- Including in terms of engagement 2.72
- Management's responsibility to assist in service auditor's use of 2.26
- Nature, timing, and extent of procedures 3.168
- Operating effectiveness of controls 3.169
- Planning to use 2.112, 2.132–153
- Professional judgment of service auditor in 2.145–147, 3.170, 3.175
- Reperformance testing in ... 3.167–168, 4.26
- Reporting on results of tests of controls 4.23–27

INTERNAL CONTROL OVER FINANCIAL REPORTING (SOC 1[®] EXAMINATION) 1.60–61, Appendix B**IT PROCESSING, TESTS OF AUTOMATED CONTROLS 3.138****L****LAWS OR REGULATIONS, COMPLIANCE WITH**

- Noncompliance issues in examination 2.122, 3.158, 3.163, 3.190–196
- Service organizations objectives and 1.44
- Written representations 3.201

M**MANAGED SECURITY, DEFINED 1.02****MANAGEMENT ASSERTIONS. See also written assertions**

- Additional subject matters and criteria ... 1.51
- Components of 1.16, Table 1-1 at 1.18
- Illustrative examples Appendix D, Appendix E, Appendix F
- Modification due to misstatements or deficiencies 3.226–229, 4.38
- Reasonable basis for, determining 2.26, 2.49–56
- SOC 3[®] report 1.56, 4.111, 4.112–114
- Subsequent event effects 3.213–219

MANAGEMENT OF SERVICE ORGANIZATION

- Additional subject matters and criteria for service auditor 1.51
- Agreement with service auditor on intended users 1.08
- Changes to the system during the period 3.62
- Communication of user entity responsibilities 3.38–41
- Description of the system from ... 1.16, 2.26, 2.117
- Design of controls 3.80
- Disclosure requirements to service auditor 2.26
- Distribution of service auditor's report by 1.13, 4.91–93

MANAGEMENT OF SERVICE**ORGANIZATION—continued**

- Information for Appendix A
- Privacy disclosures 2.61
- Response to deviations in tests of controls 4.20–21
- Responsibilities in SOC 2® examination 1.16, 1.32, 1.45, 2.03–29, 2.117, 3.13, Appendix A, Table 4-3 at 4.32
- Responsibilities in SOC 3® examination 2.167–171
- Risk identification by 1.42, 2.26, 2.52–53
- Role in use of other practitioner 2.157
- Changes in terms of engagement 2.75, 4.57
- Subservice organization evaluation by 2.98
- Written representations. See written representations

MANAGEMENT OF SUBSERVICE ORGANIZATION

- Identification of controls for implementation 2.24–25
- Responsibilities of 2.28, 2.101

MANAGEMENT OF USER ENTITY OR BUSINESS PARTNER, INTEREST IN SERVICE ORGANIZATION'S CONTROLS.

See also user entities 1.01–04

MATERIAL DEFICIENCIES

- Extended or modified period covered by examination 2.83
- Operating effectiveness of controls 4.83–88
- Suitability of design of controls 4.79–82

MATERIAL MISSTATEMENT, RISK OF

- Concluding on sufficiency and appropriateness of evidence 4.05–06
- Considering uncorrected description misstatements and deficiencies 4.10, 4.68–78
- Due to fraud. See fraud consideration
- Modified opinion type Table 4-4 at 4.47
- Performing the examination 3.01–04
- Planning the examination 2.111, 2.120–126
- Revising the risk assessment 3.181

MATERIALITY

- Adverse opinion basis 4.54–55
- Description of service organization's system 3.07, 3.72–78
- Evaluating suitability of design and operating effectiveness of controls 3.161–3.165
- Considerations during planning ... 2.104–109
- Reporting results of tests of controls 4.16
- In responding to assessed risks and planning procedures 3.05–08

MEASURABILITY, IN DESCRIPTION OF THE SYSTEM 4.71**MISSTATEMENTS. See also material misstatement, risk of**

- Defined 3.09
- Identifying and evaluating 3.09–11, 3.64–71, 3.184–189, 3.193–196
- Pervasive effects on subject matter 3.186–187, 4.45, 4.54, 4.58
- Responding to other information included with auditor's report 4.102, 4.104
- Uncorrected 3.193–196, 4.10–12, 4.68–78

MODIFICATIONS TO SERVICE AUDITOR'S REPORT (SOC 2®) 4.43–88,

- Table 4-4 at 4.47
- Adverse opinion 3.29, 4.14, 4.54–55
- Considering linkages among subject matters 4.14
- Criteria for 4.43–44
- Description material misstatements, illustrative separate paragraphs 4.68–78
- Disclaimer of opinion. See disclaimer of opinion
- Modified opinion 3.10, 3.11, 3.29, 3.71, 3.185, 3.189, 4.43–47
- Operating effectiveness of controls, illustrative separate paragraphs 4.83–88
- Qualified opinion 3.137, 4.14, 4.51–53, 4.59–60
- Qualitative and quantitative factors 4.50
- Scope limitation 4.56–60, 4.82, 4.85, Table 4-4 at 4.47
- SOC 3® report 4.118
- Suitability of controls, illustrative separate paragraphs 4.79–82
- Testing of controls 3.119

N**NONCOMPLIANCE WITH LAWS OR REGULATIONS 2.122, 3.190–196****O****OPERATING EFFECTIVENESS OF CONTROLS (TYPE 2 EXAM). See also tests of controls 3.106–146**

- Considering request to extend or modify period 2.80
- Controls not operating during examination period 3.156
- Deficiencies distinguished from those for design of controls 3.102
- Deviations in, identifying and evaluating 3.157–160
- Entity-level controls 2.127–131
- Impact of suitability of design of controls on 3.109
- Internal audit function, using work of 3.169
- Material deficiencies noted in service auditor's report 4.83–88

**OPERATING EFFECTIVENESS OF CONTROLS
(TYPE 2 EXAM)—continued**

- Materiality considerations 3.162, 3.164
- Monitoring as internal control function 2.119
- Scope limitation, illustrative separate paragraphs 4.85
- Service auditor's engagement requirements 1.06, 1.17
- Subservice organizations ... 3.81, 3.153–154
- Superseded controls in ... 3.108, 3.140–141
- Trust services criteria ... 1.32–35, 1.40–43, 3.107, Table 1-2 at 1.41

OPINION, SERVICE AUDITOR'S

- Adverse 3.29, 4.14, 4.54–55
- Disclaiming of. *See* disclaimer of opinion
- Evaluating the results of procedures performed 3.183
- Extended or modified period consideration 2.84
- Forming the opinion for service auditor's report 4.04–14, Table 4-3 at 4.32
- Illustrative Appendix D
- Modified. *See also* modifications to service auditor's report 3.10, 3.11, 3.29, 3.71, 3.185, 3.189, 4.43–47, 4.118
- Qualified ... 3.137, 4.14, 4.51–53, 4.59–60
- Service auditor's engagement requirements 1.06, 2.64
- SOC 3[®] report 1.13, 4.111, 4.115, Table 4-4 at 4.116
- Type 1 and type 2 SOC 2[®] requirements Table 1-1 at 1.18

**OTHER-MATTER PARAGRAPHS, IN SERVICE
AUDITOR'S REPORT 4.89–90****OTHER PRACTITIONER, USING WORK
OF 2.154–159, 4.42****OUTSOURCING. *See also* subservice
organizations 1.01–02, 2.06****P****PEOPLE, AS SYSTEM COMPONENT 1.20****PERFORMING A SOC 2[®]
EXAMINATION 3.01–229**

- Applicable trust services criterion, multiple controls for 3.92–94
- Business partner and vendor risks 3.147–151
- Changes to the system during period covered by type 2 exam 3.55–56, 3.62, 3.108, 3.140–141
- Changes to the system occurring between periods covered by type 2 exam ... 3.57–58
- Controls not operating during examination period 3.156
- CUECs and user entity responsibilities 3.36–41

**PEOPLE, AS SYSTEM
COMPONENT—continued**

- Deficiencies in controls 3.101–105, 3.193–196
- Description of the system, evaluating and obtaining evidence 3.12–78
- Design of controls, evaluating suitability of 3.79–105
- Deviations in controls 3.157–160
- Disclosures about individual controls 3.30–32, Table 3-1 at 3.30
- Documentation 3.221–225
- Fraud consideration 3.190–196
- Internal audit function, using work of 3.166–177
- Management assertions, need for modification in 3.226–229
- Materiality considerations 3.05–08, 3.72–78, 3.161–165
- Misstatements, identifying and evaluating 3.09–11, 3.64–71, 3.184–189, 3.193–196
- Noncompliance with laws or regulations 3.190–196
- Operating effectiveness of controls. *See also* tests of controls 3.106–146, 3.153–154, 3.156–165
- Reliability of information produced by service organization, evaluating 3.121–130
- Responding to and communicating resulting issues 3.190–196
- Results of procedures, evaluating 3.182–189
- Revising the risk assessment 3.181
- Service commitments and system requirements 3.24–29
- Specialist, using work of 3.178–180
- Subsequent events and subsequently discovered facts 3.213–220
- Subservice organizations 3.42–54, 3.88–91, 3.99–100, 3.152–155
- Suitability of design of controls, evaluating 3.79–105
- Uncorrected misstatements 3.193–196
- Written representations, obtaining from management 3.197–212

PERIODS. *See also* subsequent events

- Changes to the system between ... 3.57–58
- Changes to the system during 3.55–56, 3.62, 3.108, 3.140–141
- Controls that did not operate during ... 3.156
- Controls not suitably designed during portion of period 4.81
- Date of service auditor's report Table 4-3 at 4.32, Table 4-4 at 4.116
- Evidence from prior periods, in tests of controls 3.136–137

PERIODS—continued

- Extending or modifying the period covered by the examination 2.79–90
- Interim tests of controls 3.132
- Threats related to prior periods 3.163

PLANNING A SOC 2®**EXAMINATION 2.91–166**

- Entity-level controls consideration 2.127–131
- Inclusive method for presenting services of subservice organization 2.96–103
- Internal audit function, understanding and planning to use 2.112, 2.132–153
- Materiality consideration 2.104–109
- Other practitioner, using work of 2.154–159
- Performing risk assessment procedures 2.110–126
- Service auditor's specialist, using work of 2.160–166
- Strategy for examination 2.91–95

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS. See service commitments and system requirements**PRIOR ENGAGEMENTS, EVIDENCE FROM 3.137****PRIVACY**

- Applicable trust services criteria Table 1-2 at 1.41, Supplement B
- Boundaries of the system and 1.22
- Confidentiality distinguished from 1.25–26
- Defined 1.37
- Service organization controls relevant to 1.04
- Service organization management disclosures relevant to 2.61

PROCESSING INTEGRITY

- Applicable trust services criteria Table 1-2 at 1.41, Supplement B
- Boundaries of the system and 1.22
- Defined 1.22, 1.37
- Service organization controls relevant to 1.04

PROFESSIONAL JUDGMENT

- Engagement acceptance and continuance 2.77
- Extent of sampling in tests of controls 3.144
- Internal audit function, using work of 2.145–147, 3.170, 3.175
- Materiality consideration 2.107
- Modification of opinion basis 4.45
- Reliability of information produced by service organization 3.129
- Sufficiency and appropriateness of evidence 4.09

PROSPECTIVE USER ENTITIES OR BUSINESS PARTNERS 1.10**Q****QUALIFIED OPINION 3.137, 4.14, 4.51–53, 4.59–60****QUALITATIVE AND QUANTITATIVE FACTORS**

- In modifications to the service auditor's report 4.50
- Suitability of design of controls, evaluating 3.163–164

QUALITY CONTROL**CONSIDERATION ... 1.74–76, 2.31–34, 2.39–42****R****REASONABLE BASIS FOR MANAGEMENT****ASSERTION, DETERMINING 2.26, 2.49–56****REGULATORS, AS SPECIFIED PARTIES IN SERVICE ORGANIZATION****RELATIONSHIP 1.09****REPERFORMANCE TESTING, IN USING THE****WORK OF THE INTERNAL AUDIT FUNCTION! 3.167–168, 4.26****REPORT USERS, DEFINED. See also intended users 3.12****REPORTING. See service auditor's report****REPRESENTATION LETTER. See written representations****RESPONSIBLE PARTY**

- Independence of service auditor in relation to 2.37
- Subservice organization as. See also management of service organization ... 2.96
- Written representation from engaging party that is not 3.212

RESTRICTIONS ON USE OF SERVICE AUDITOR'S REPORT

- SOC 2® report 1.11–12, 4.33–35, 4.91–93
- SOC 3® report 4.117

RISK ASSESSMENT

- Entity-level controls 2.127–131
- Expected knowledge of intended users and 1.08
- Generally 1.03–04
- Material misstatement, risk of. See material misstatement, risk of
- Planning SOC 2® examination procedures 2.104–126
- Revising 3.181
- Service auditor's evaluation of 3.82–84
- Business partners and vendor risk 3.147–151
- By user entity management 1.04

S

SAMPLING. See audit sampling**SCOPE OF ENGAGEMENT**

- Information not covered by service auditor's report 4.95–104
- Change in terms of examination 2.75
- Modifications to service auditor's report due to limitation on 4.56–60, 4.82, 4.85, Table 4-4 at 4.47
- Service auditor's response to limitation on 3.211, Appendix D-3
- SOC 3® Table 4-4 at 4.116

SCOPE LIMITATION

- Changed engagement 2.77
- Modify the service auditor's opinion 3.141
- Disclaim an opinion 3.192, 3.211, 4.65, Appendix D-3
- Generally 4.56-4.60,
- Related to suitability of design of controls 4.82
- Related to suitability of operating effectiveness 4.85
- SOC 3® 4.117

SECURITY

- Applicable trust services criteria Table 1-2 at 1.41, Supplement B
- Boundaries of the system and 1.22
- Defined 1.37
- Evaluating controls for 3.163
- Service organization controls relevant to 1.04

SERVICE AUDITORS

- Acceptance and continuance 2.30–2.74
- Additional subject matters and criteria procedures 1.50–54, Table 1-3 at 1.50
- Agreeing on terms of engagement 2.70–74
- Agreement with management on intended users 1.08
- Changes to terms of engagement, considering 2.75–78
- Confidentiality in regard to client information 3.195–196
- Considering request to extend or modify period 2.79–85
- Documentation responsibilities of 3.222
- Engagement requirements in type 2 examination 1.06, 1.17
- Independence of. See independence of service auditors
- Opinion from. See opinion
- Performing the examination. See performing a SOC 2 examination
- Planning the examination 2.91–126
- Professional judgment. See professional judgment
- Reporting responsibilities of. See also service auditor's report 4.01–03, Table 4-3 at 4.32

SERVICE AUDITORS—continued

- Responsibilities of, generally 1.17, 2.30
- SOC 3® examination responsibilities 2.172
- Subsequent event responsibilities 3.215–217
- Tests of controls responsibilities 1.53, 3.110, 3.115–120
- Withdrawal from engagement 2.68, 2.78, 3.229

SERVICE AUDITOR'S ENGAGEMENTS**SERVICE AUDITOR'S REPORT (SOC 2®). See also SOC 1® examination and report; SOC 3® report 4.01–116****Additional subject matters and**

- criteria 1.52–54, Table 1-3 at 1.50**
- Assessing usefulness of separate reports 2.114
- Carve-out method at subservice organization 4.32, 4.39–41, Appendix D-1
- Contents of Table 1-1 at 1.18
- On controls not operating during reporting period 3.156
- CUECs 4.36–38
- Date of report Table 4-3 at 4.32
- Defined 1.04
- Determining appropriateness for intended users 2.47–48
- Disclaims an opinion because of a scope limitation Appendix D-3
- Distribution of report by management 4.91–93
- Elements of 4.31–32, Table 4-3 at 4.32
- Emphasis-of-matter and other-matter paragraphs 4.89–90
- Forming the opinion. See also opinion, service auditor's 4.04–14
- Information accompanying but not covered by 4.95–104
- Inclusive method, illustrative report Appendix D-2
- Illustrative type 2 report, Appendix D-4
- Intended users of 1.07–13
- Internal audit function, using work of 4.23–27
- Materiality in 4.16, 4.54–55
- Modifications to. See modifications to service auditor's report
- Other practitioner in 2.156, 4.42
- Recommendations for improving controls 4.94
- Describing tests of reliability of information produced by service organization 4.28–30
- Responsibilities of service auditor ... 4.01–03
- Restrictions on use of report 1.11–12, 4.33–35, 4.91–93
- Risk assessment 1.04

Additional subject matters and criteria—continued

- SOC 3[®] reports distinguished from 1.55–57
- Tests of controls and results of tests 4.15–30, 4.42, Table 4-1 at 4.15, Table 4-2 at 4.17, Table 4-3 at 4.32
- Type 1 and type 2. See type 1 SOC 2[®] examination and report; type 2 SOC 2[®] examination and report

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

- In description of the system 1.44–1.49, 2.59–65, 3.24–29, Appendix D
- Evaluating appropriateness in accepting engagement 2.59–65
- Generally 1.44–49, 2.04
- Management responsibility for 2.04, 3.13
- Relevance of controls to achievement of 3.163
- SOC 3[®] report 4.112, 4.115

SERVICE ORGANIZATIONS 1.01–77

- Commitments to user entities. See also service commitments and system requirements 1.44–46, 1.49
- Controls responsibilities 1.40
- Defined 1.01
- Description. See description of service organization's system
- Management of. See management of service organization
- Other information accompanying auditor's report 4.95–104
- Outsourcing. See also subservice organizations 1.01
- System. See system, service organization's
- Types of services provided 1.02
- User entities 1.01–13

SOC 1[®] EXAMINATION AND REPORT (SOC FOR SERVICE ORGANIZATIONS: ICFR) 1.60–61, Appendix B**SOC 2[®] EXAMINATION. See also performing a SOC 2[®] examination; service auditor's engagements**

- Accepting an engagement. See accepting a SOC 2[®] examination engagement
- Additional subject matter and additional criteria 1.50–54, Table 1-3 at 1.50
- Applicable trust services criteria 1.05, 1.08, 1.27, Table 1-1 at 1.18, Supplement B
- Boundaries of the system and 1.21–23
- Categories of criteria 1.37–38, 1.41, 4.76, Table 1-2 at 1.41
- Common criteria 1.39–43, Table 1-2 at 1.41
- Criteria for. See also description criteria; trust services criteria 1.27–43

SOC 2[®] EXAMINATION—continued

- Cybersecurity risk management examination and report, distinguished from ... Appendix C
- Defined 1.04
- Distinguishing between confidentiality and privacy 1.25–26
- Overview of 1.14–49
- Performing the examination. See performing a SOC 2[®] examination
- Planning the examination. See planning a SOC 2[®] examination
- Professional standards applicable to 1.69–76
- Scope of and boundaries of the system 1.23
- Scope of as set by management 2.04
- System definition 1.19–20
- Time frame of 1.24
- Trust services criteria. See trust services criteria
- Type 1 distinguished from type 2 ... 1.05–06, 1.14, 1.16–17
- Use of SOC 2[®] reports internationally, Appendix H

SOC 2[®] REPORT. See service auditor's report**SOC 3[®] EXAMINATION**

- Generally 1.55–58
- Management's responsibilities 2.167–171
- Service auditor's responsibilities 2.172
- SOC 2[®] engagements distinguished from 1.55, Appendix B

SOC 3[®] REPORTS

- Elements of 4.110–116, Table 4-4 at 4.116
- Illustrative report Appendix F
- Management assertion, illustrative Appendix F
- Modification of opinion on effectiveness of controls 4.118
- Restricting distribution of 4.117
- SOC 2[®] reports distinguished from 1.55–57, Appendix B

SOC FOR CYBERSECURITY 1.63–68**SOC SUITE OF SERVICES 1.59–68****SOFTWARE, AS SYSTEM COMPONENT 1.20****SPECIALIST, USING WORK OF 2.160–166, 3.178–180****SPECIFIED PARTIES. See intended users****SUBJECT MATTERS OF A SOC 2[®] EXAMINATION**

- Addressing additional 1.50–54, Table 1-3 at 1.50
- Description of the system. See description of service organization's system
- Design of controls. See suitability of design of controls

SUBJECT MATTERS OF A SOC 2[®]**EXAMINATION—continued**

- Determining appropriateness of 2.44–56
- Effectiveness of controls. See operating effectiveness of controls
- Evaluating pervasive effects of misstatements on 3.186–187, 4.45, 4.54, 4.58
- Expressing the opinion on 4.13–14
- Generally 1.05
- Management's written representations on 3.201, 3.205
- Service auditor's exam responsibilities ... 3.11
- Service auditor's report Table 4-3 at 4.32

SUBSEQUENT EVENTS AND SUBSEQUENTLY DISCOVERED FACTS 3.213–220**SUBSERVICE AUDITOR, USING WORK OF 2.157****SUBSERVICE ORGANIZATIONS**

- Auditor independence from 2.15, 2.37
- Carve-out method. See carve-out method
- Controls of 2.06–10, 3.43–54
- Defined 2.06–07
- In description of the system 2.11–16, 2.24–25, 3.42–54, 4.75
- Identification of complementary controls by service organization's management 2.17–19
- Identification of controls for service organization to implement 2.24–25
- Illustrative auditor's reports Appendix D
- Inclusive method. See inclusive method
- Management responsibilities of ... 2.28, 2.101
- Not disclosed in description of the system, illustrative separate paragraph 4.75
- Operating effectiveness of controls, evaluating 3.81, 3.153–154
- Planning for multiple 2.97
- As responsible parties 2.96
- In risk assessment 2.123, 3.82
- Service auditor's report Table 4-3 at 4.32
- Service organization management's identification and evaluation of ... 2.06–11, 2.98
- Suitability of design of controls, evaluating 2.16, 3.86, 3.88–91, 3.99–100, 3.152
- Written assertions 2.28, 2.100, 2.103
- Written representations 2.28, 3.206

SUITABILITY OF CRITERIA, ASSESSING. See also description criteria; trust services criteria 2.57–58**SUITABILITY OF DESIGN OF CONTROLS 3.79–105**

- Multiple controls to address applicable trust services criteria 3.92–94, 3.114
- CUECs and 3.86, 4.36–38
- Deficiencies, identifying and evaluating 3.101–105, 4.79–82

SUITABILITY OF DESIGN OF CONTROLS—continued

- Defined 1.34
- Fraud consideration 3.86, 3.162
- Generally 3.79–87
- Illustrative separate paragraph 4.82
- Impact on evaluation of operating effectiveness of controls 3.109
- Intentional and unintentional acts in ... 3.163, 3.190
- Materiality considerations 3.104, 3.161–165
- Not suitably designed, illustrative separate paragraph 4.79–82
- Procedures to obtain evidence 3.95–100
- Qualitative and quantitative factors 3.163–164
- Service auditor's engagement requirements 1.06
- Subservice organizations 2.16, 3.86, 3.88–91, 3.99–100, 3.152
- Trust services criteria ... 1.32–35, 1.40–43, 3.94, Table 1-2 at 1.41
- Unknown threats and vulnerabilities 3.163

SUPERSEDED CONTROLS, IN OPERATING EFFECTIVENESS OF CONTROLS EVALUATION 3.108, 3.140–141**SYSTEM**

- Boundaries of the system 1.21–23, 2.45, 2.113, 3.32
- Changes between periods 3.57–58
- Changes during the period ... 3.55–56, 3.62, 3.108, 3.140–141
- Components of 1.20
- Controls for. See controls
- Defined 1.19–20
- Description of. See description of service organization's system
- Objectives for 1.44
- Obtaining an understanding of ... 2.110–119
- Requirements of. See service commitments and system requirements

SYSTEM AND ORGANIZATION CONTROLS (SOC). See SOC Suite of Services**SYSTEM INCIDENT DISCLOSURES 3.33–35****T****TERMS OF ENGAGEMENT**

- Agreeing on for a SOC 2[®] engagement 2.32, 2.70–90
- Changes in 2.75–78

TESTS OF CONTROLS 3.110–146

- Audit sampling 3.142–146
- Designing and performing 3.110–114

TESTS OF CONTROLS—continued

- Deviations and deficiencies
 - analysis 3.157–160, 3.185–189
- Extent of 3.134–139, 4.18
- Internal auditor, using work of ... 3.167–168, 4.23–27
- Nature of 3.115–120
- Reliability of information produced by service organization 3.121–130
- Reporting tests and results in type 2 report ... 4.15–30, 4.42, Table 4-1 at 4.15, Table 4-2 at 4.17, Table 4-3 at 4.32
- Service auditor's responsibilities 1.53, 3.110, 3.115–120
- Superseded controls 3.140–141
- Timing of 3.131–133
- Type of control and best procedure to test 3.118

TRUST SERVICES CATEGORIES. See also specific categories by name 1.37–38, 1.41, 1.46, 4.76, Table 1-2 at 1.41

TRUST SERVICES CRITERIA Supplement B

- Applicable trust services criteria ... 1.05, 1.32, 3.92–94, 4.77, Table 1-2 at 1.41, Table 4-4 at 4.116, Supplement B
- Assessing suitability of 2.57–58
- Categories 1.37-1.38
- Common criteria 1.39-1.42
- Confidentiality criteria 1.25–26
- Description of the system including irrelevant data, illustrative separate paragraph 4.87–88
- Generally 1.05, 1.08, 1.27, 1.31–36, Supplement B
- Multiple controls to address an applicable trust services criterion ... 3.92-94
- Operating effectiveness of controls ... 1.32–35, 1.40–43, 3.107, Table 1-2 at 1.41
- Privacy criteria 1.25–26
- Resource for Supplement B
- Service commitments and system requirements 2.63–64
- Suitability of design of controls ... 1.32–35, 1.40–43, 3.94, Table 1-2 at 1.41

TYPE 1 SOC 2® EXAMINATION AND REPORT

- Contents of 4.107–109, Table 1-1 at 1.18, Appendix E
- Time frame for examination 1.24
- Type 2 SOC 2® examination distinguished from 1.05–06, 1.14, 1.16–17

TYPE 2 SOC 2® EXAMINATION AND REPORT. See also service auditor's report

- Changes to the system occurring between periods 3.57–58
- Contents of Table 1-1 at 1.18

TYPE 2 SOC 2® EXAMINATION AND REPORT—continued

- Defined 1.05
- Extending or modifying the period covered by 2.79–90
- Illustrative 4.105–106, Appendix D
- Operating effectiveness of controls. See operating effectiveness of controls
- System changes implemented during the period 3.62, 3.108, 3.140–141
- Tests of controls. See tests of controls
- Time frame for examination 1.24
- Type 1 SOC 2® examination distinguished from 1.05–06, 1.14, 1.16–17

U**USER ENTITIES**

- Boundary of the system, clarity of reporting on 1.21
- Business relationships with service organizations ... 1.01–13
- Categories of 1.09
- Controls. See complementary user entity controls
- Defined 1.01
- Management of 1.04
- Prospective 1.10
- Responsibilities of 1.03, 1.08, 2.20–23, 3.36–41
- Risk assessment 1.04
- Service commitments and system requirements 1.44–1.49, 2.59–65, 3.24–29

V**VENDOR AND BUSINESS PARTNER RISKS, CONSIDERATION OF. See also subservice organizations** 3.147–151**W****WRITTEN ASSERTIONS. See also management assertions**

- To accompany description of service organization system 2.26
- Elements of 1.16
- Management refusing to provide 2.68, 4.64–67
- Requesting of service organization management 2.66–69
- SOC 3® report 1.56
- From subservice organization's management 2.28, 2.100, 2.103

WRITTEN REPRESENTATIONS ... 3.197–212

- At conclusion of engagement 2.26
- For extended or modified period 2.86
- Illustrative examples Appendix G

WRITTEN REPRESENTATIONS—continued

- Management's refusal to provide 3.211,
..... 4.66
- Not provided or not reliable 3.209–.211
- Requesting of service organization
management 2.66–69

WRITTEN REPRESENTATIONS—continued

- On subject matters of the
examination 3.201, 3.205
- Subservice organizations 2.28, 3.206
- When engaging party is not responsible
party 3.212

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>

<http://www.pbookshop.com>