NAVIGATING CHANGES TO THE SOC 2 GUIDE

January 17, 2023

CPE Placeholder

DELETE AND REPLACE WITH MEDIA SPECIALIST CPE SLIDE

With You Today

BINITA PRADHAN
Partner

bpradhan@bdo.com

TIM SEIGLER
Principal

tseigler@bdo.com

JASON LIPSCHULTZ
Partner

jlipschultz@bdo.com

MICHAEL DEEMING
Managing Director

mdeeming@bdo.com

Agenda

SOC 2 Guide Overview

Summary of Changes

Next Steps

Questions

SOC 2 Guide Overview

Overview

SOC 2 reports are issued to achieve the service organization's service commitments and system requirements based on predefined criteria for one or more of the trust services criteria set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) (AICPA, Trust Services Criteria).

The AICPA has provided specific guidance in performing SOC 2 reports, and these reports are performed using the AICPA Guide: SOC 2® Reporting on an Examination of Controls at a Ser-vice Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy. SOC 2 reports specifically address one or more of the following five categories:

1. **Security**
2. **Availability**
3. **Processing Integrity**
4. **Confidentiality**
5. **Privacy**

SOC 2 GUIDE

Overview

In late October 2022, the American Institute of Certified Public Accountants' (AICPA's) Assurance Services Executive Committee (ASEC) released an update to the System and Organization Control (SOC) 2 reporting guide. Significant updates have been made to the **Description Criteria implementation guidance** and the **Trust Services Criteria points of focus.** Overall, the changes provide clarity around several recent and emerging industry topics and continue to promote reporting quality and consistency.

Summary of Changes

MICHAEL

SOC 2 GUIDE

Change Overview

Available for use now, the AICPA updates for SOC 2 examinations are significant and may require additional time and attention from companies who currently have a SOC 2 report or are planning on working toward compliance.

IN SUBSEQUENT SLIDES WE WILL COVER THE FOLLOWING:

Learning specific, key changes made to the SOC 2 guide	Understanding the purpose and benefit of the changes to the SOC 2 guide	Obtaining practical guidance on how to apply these changes to your control environment

SOC 2 GUIDE

Change Overview

IN SUBSEQUENT SLIDES WE WILL COVER THE FOLLOWING:

- Updates to the AT-C Sections and relevant SSAEs
- Changes to Description Criteria Implementation Guidance
- Changes to points of focus

SUMMARY OF CHANGES

Professional Standards Governing Engagements Using the Trust Services Criteria

Incorporating new attestation standards (e.g., SSAE 19 and SSAE 21).

Examination engagements and engagements to apply agreed-upon procedures performed in accordance with Statements on Standards for Attestation Engagements (SSAEs) may use the trust services criteria as the evaluation criteria. The SSAEs provide guidance on performing and reporting in connection with examination, review, and agreed-upon procedures engagements.

CURRENT RELEVANT SSAE GUIDANCE FOLLOWS:

- AT-C section 105 (Concepts Common to All Attestation Engagements): SSAE No. 19; SSAE No. 21
- AT-C section 205 (Assertion-Based Examination Engagements): SSAE No. 21 supersedes SSAE No. 18
- AT-C section 206 (Direct Examination Engagements): SSAE No. 21 new for direct engagements
- AT-C section 215 (Agreed-Upon Procedures Engagements): SSAE No. 19 supersedes SSAE No. 18

SUMMARY OF CHANGES

Implementation Guidance for Description Criteria

Updates to the Description Criteria implementation guidance for additional clarity regarding certain disclosure requirements, guidance on disclosure of how controls meet the requirements of a process or control framework, and guidance on disclosure of information about the risk assessment process and specific risks.

DESCRIPTION CRITERIA DISCLOSURE UPDATES:

- **DC1:** The types of services provided
- **DC2:** The principal service commitments and system requirements
- **DC3:** The components of the system used to provide the services, including the following:
  A. Infrastructure
  B. Software
  C. People
  D. Procedures
  E. Data

SUMMARY OF CHANGES

Implementation Guidance for Description Criteria

Updates to the Description Criteria implementation guidance for additional clarity regarding certain disclosure requirements, guidance on disclosure of how controls meet the requirements of a process or control framework, and guidance on disclosure of information about the risk assessment process and specific risks.

DESCRIPTION CRITERIA DISCLOSURE UPDATES:

- **DC4:** For identified system incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements…
- **DC5:** The applicable trust services criteria and the related controls
- **DC6:** Complementary user entity controls (CUECs)

SUMMARY OF CHANGES

Implementation Guidance for Description Criteria

Updates to the Description Criteria implementation guidance for additional clarity regarding certain disclosure requirements, guidance on disclosure of how controls meet the requirements of a process or control framework, and guidance on disclosure of information about the risk assessment process and specific risks.

DESCRIPTION CRITERIA DISCLOSURE UPDATES:

- **DC7:** When the service organization uses a subservice organization and the controls at the subservice organization are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved
- **DC8:** The applicable trust services criteria relevancy
- **DC9:** Relevant details of significant changes to the service organization's system and controls during that period that are relevant to the service organization's service commitments and system requirements

SUMMARY OF CHANGES

Points of Focus

Updates to the points of focus that support the application of the Trust Services Criteria that better reflect the ever-changing technology, legal, regulatory, and cultural risks, data management requirements, particularly related to confidentiality, and differentiating between a data controller and a data processor for privacy engagements.

NUMEROUS UPDATES TO POINTS OF FOCUS, SEVERAL TO NOTE:

- **CC2.1:** Additional points for data integrity
- **CC3.4:** Assesses Changes in Threats and Vulnerabilities
- **CC6.3:** Reviews Access Roles and Rules
- **CC6.6:** Restricts Access
- **CC8.1:** Manages Patch Changes
- **CC9.2:** Identifies Vulnerabilities

Summary of Changes

JASON

SOC 2 GUIDE

Change Overview

IN SUBSEQUENT SLIDES WE WILL COVER THE FOLLOWING:

- Making qualitative materiality assessments
- Use of software applications and tools
- Controls that may operate outside the reporting period

Summary of Changes

Making qualitative materiality assessments (from the AICPA whitepaper on materiality).

- Meeting the common needs of a broad range of users
- Mainly qualitative in nature
  - Relevant disclosures, including ‘Emphasis of Matter’
  - Impact of control deficiencies on the Description
  - Compliance with laws and regulations
  - Potential misstatements
- Description's impact on judgments made by users, including any inadvertent errors and omissions

Summary of Changes

Considering the service organization's use of software applications and tools (from the SOC Tools FAQ).

- Appropriate use of, and reliance on, software tools
- Clear delineation between software vendors and service auditors
- Full inventory of all applications AND tools used to support the operation of controls, including:
  - Reporting tools
  - Incident management tools
  - Control automation platforms
- Vendor or SSO?
- Controls in place over the tools
- Data generated by these tools utilized in the operation of controls

Summary of Changes

Considering the operation of periodic controls that operated prior to the period covered by the examination.

- Relevance and significance of the control to meet the criteria and achieve service commitments and system requirements
- Nature, timing, and extent relative to the reporting period
- Impact on other controls
- History of control design and operating effectiveness
- Changes in the control environment
- Potential impact on the opinion

Summary of Changes

TIM

SOC 2 GUIDE

Change Overview

IN SUBSEQUENT SLIDES WE WILL COVER THE FOLLOWING:

- Use of specialists
- SOC 2+
- Website updates

Summary of Changes

Considering management's use of specialists.

- Considerations for reporting lines and potential independence considerations related to use of specialists
- Are specialists operating controls and/or how are these lines of oversight reported within the organizational structure
  - Should these be potential subservice organizations?
- Utilization of compelling audit evidence

Summary of Changes

Performing and reporting in a SOC 2+ engagement (including an updated illustrative service auditor's report).

- Additional Subject Matter Considerations:
- Description Criteria Updates
  - **.09/DC-2/DC-3** – No specific templates for inclusion within Process Narrative, but should be appropriately described including necessary boundaries of the additional criteria (does not include operating effectiveness example within template – for auditor determination)
  - **DC-8** – Are all components of the additional subject matter applicable?

Summary of Changes

Addressing considerations when the service organization has identified a service commitment or system requirement related to meeting the requirements of a process or control framework (such as HIPAA, ISO or NIST).

- Beneficial for leveraging one reporting mechanism for multiple frameworks
- Should be included within the description including necessary updates to opinion if tested as additional criteria (vs. Mapping to SOC 2 within other information section)

Summary of Changes

Supplements and several appendices were removed and will be replaced with links to the appropriate documents on the AICPA website.

- Intention to streamline approach to finding the relevant portions of the guide on the AICPA website

Next Steps

What Does This Mean for Organizations?

If you currently have or will be working toward a SOC 2 report, it's essential to understand the impact to the SOC 2 reporting process. Early preparation will help your organization stay ahead of the curve when it comes to preparation and achieving compliance.

PLAN

- Obtain the new guide
- Review to understand changes
- Ensure updates are communicated to stakeholders
- Coordinate with auditors on the planned timing for any upcoming audits

IMPLEMENT

- Map your controls considering the new implementation guidance related to the Description Criteria and Trust Services Criteria;
- Identify any reporting gaps to determine any necessary incremental controls and system description updates;
- Consider if updates to mapping with other frameworks necessary

ASSESS

- Update policies, procedures, and documentation
- Enhance control activities as appropriate
- Perform internal audit using 2022 guidance
- Develop a SOC 2 reporting plan incorporating the new requirements

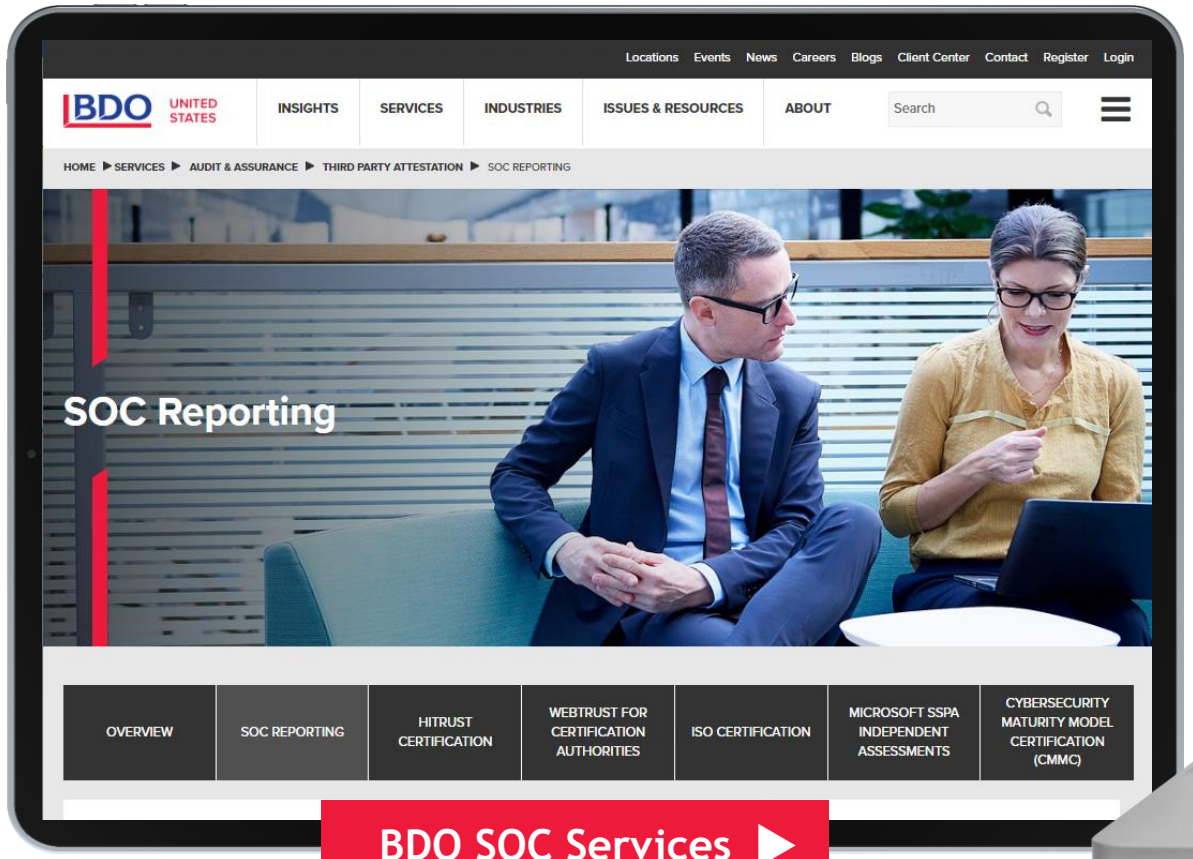
SOC 2 Guidance Change Observations

The updated guidance benefits SOC 2 reporting stakeholders in the following ways:

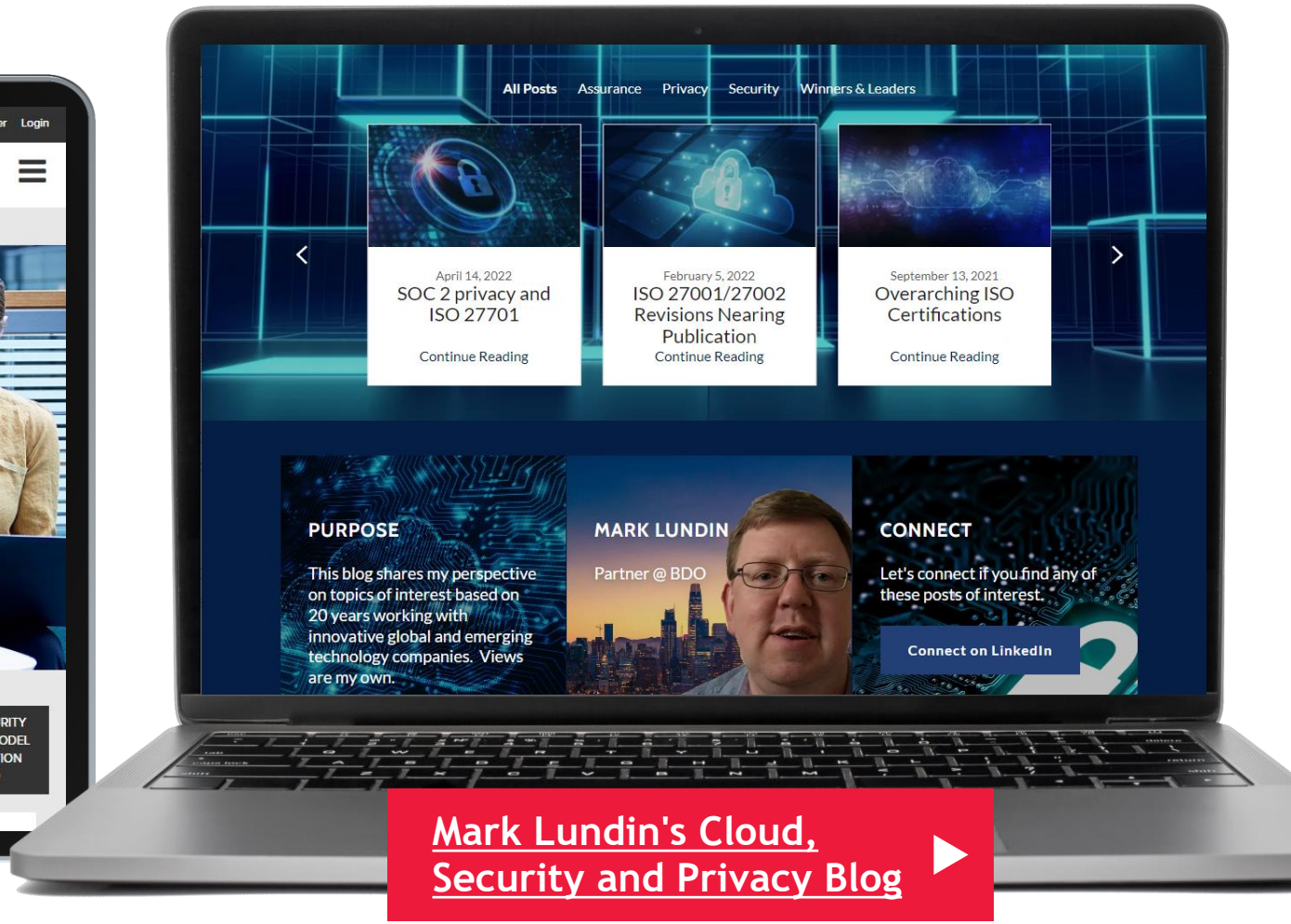
- Clarifications should enhance consistency in reporting;
- The 2018 Description Criteria did not change, however revised implementation guidance presents important factors to consider when making judgments about the nature and extent of disclosures called for by each criterion;
- Revised Points of Focus provide additional activities to consider when addressing Trust Services Criteria;
- Organizations should work closely with their auditors to consider opportunities to enhance their reporting.

Questions?

Resources



BDO SOC Services



Mark Lundin's Cloud, Security and Privacy Blog

Thank You!

About BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com