May 6, 2022

The Honorable Gary Gensler, Chair
U.S. Securities and Exchange Commission

Re: Request for Comment on Proposed Rule, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* [Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

Dear Chair Gensler:

The American Institute of CPAs (AICPA) is pleased to respond to the US Securities and Exchange Commission's (SEC or Commission) request for comment on the Proposed Rule, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (Proposed Rule). We appreciate the opportunity to help inform the SEC's rule-making process.

We support the SEC's efforts to strengthen cybersecurity disclosures in response to rapidly evolving marketplace needs. We have drafted this letter to provide some background and context to the Commission regarding the CPA profession's efforts in the cybersecurity space, which we believe will provide a common foundation for meaningful cybersecurity risk management and reporting to support decision-making by investors and other stakeholders.

Overall View

As you know, in today's global markets, new cybersecurity threats loom over all public, private, not-for-profit, and governmental organizations, regardless of the industries or countries in which they operate. The World Economic Forum's *Global Risks Report 2021* recognized that cybercrimes are "increasingly sophisticated and frequent, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability." In fact, that report identifies the failure of current cybersecurity measures among risks with the highest likelihood of occurrence within the next ten years. [1] When coupled with unidentified vulnerabilities in new and emerging technologies, cybersecurity risk is top of mind for all organizations.

Investors and other stakeholders need access to timely, transparent, and decision-relevant disclosures about matters beyond the financial statements. The SEC recognized investors' need for consistent, comparable, and reliable information about an organization's environmental, social, and governance (ESG) efforts in its recent proposed rules mandating certain climate-related financial statement metrics and related disclosures. [2] Similarly, many investors and other stakeholders have also identified the need for comparable, reliable, and decision-relevant disclosures about the cybersecurity risks of organizations, and most importantly how organizations identify, assess, and mitigate those risks.

---

[1] World Economic Forum, *The Global Risk Report*, page 7.

[2] SEC's proposed rules, *The Enhancement and Standardization of Climate-Related Disclosures for Investors* (March 2022)

As the SEC considers cybersecurity risk management, strategy, governance, and incident reporting, we think it is essential that all market participants work towards a comprehensive global reporting solution designed to provide investors and other stakeholders with valuable insight into the measures an organization is taking to mitigate risks and respond to cybersecurity incidents. While it is not possible to guarantee breach prevention, organizations that do not have an effective cybersecurity risk management program in place are at serious risk of being unable to meet their operational, financial, and reporting objectives, to the detriment of both short-term and long-term value creation potential.

In 2017, the AICPA created the freely available *Cybersecurity Risk Management Reporting Framework* in recognition of the growing prevalence of cybersecurity risk, and of the related need for commonly accepted, comprehensive standards for effective and transparent cybersecurity risk management and related reporting. The AICPA's *Cybersecurity Risk Management Reporting Framework* includes two distinct but complementary sets of criteria that may be used by organizations to help provide robust, decision-useful cybersecurity information to a broad range of users:

- The AICPA's *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* (Description Criteria) sets forth a list of disclosures intended to provide a description of an organization's cybersecurity risk management program. A description prepared in accordance with the description criteria provides users with information about how an organization identifies its sensitive information and systems, the ways in which the organization identifies and manages cybersecurity risks that threaten it, and a summary of processes implemented and operated to protect the information and systems against those risks.

  Similar to the SEC's proposed disclosures, the Description Criteria are designed to assist companies in reporting tailored, meaningful information that is relevant in light of the nature and circumstances in which they operate. Appendix A to this letter provides a mapping of elements of the Description Criteria to the SEC's proposed disclosures, which may serve as a useful reference to the SEC in providing registrants with helpful guidance for preparing cybersecurity disclosures should the proposed rule be implemented.

  In our view, the Description Criteria can serve as a foundation to help management and boards take a more consistent and comparable approach in establishing a cybersecurity risk management program, and in considering the nature and extent of disclosures that would be necessary for investors to understand how the company addresses cybersecurity risk. That said, since the Description Criteria were designed to meet the potential cybersecurity risk management information needs of a wide variety of stakeholders, a subset of this type of reporting is likely most relevant for investors.

- The AICPA's *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (Trust Services Criteria) are outcome-based criteria that can be used to evaluate and report on processes and controls that affect the security, availability, and processing integrity of systems and the confidentiality and privacy of the information processed by those systems. Specifically, the Trust Services Criteria covering security, availability, and confidentiality can be used to evaluate and report on an organization's cybersecurity efforts.

  The Trust Services Criteria are an extension of COSO's *Internal Control – Integrated Framework,* which is most commonly used to evaluate and report on the effectiveness of a registrant's internal control

over financial reporting in accordance with Section 404 of the Sarbanes Oxley Act. The Trust Services Criteria, like COSO, do not require organizations to implement a specific array of controls like many existing process and control frameworks do; rather, they are based on the recognition that organizations need to:

- Identify their operational, reporting and compliance requirements
- Identify the cybersecurity objectives that result from these requirements
- Identify the threats to the achievement of the objectives and the vulnerabilities of its operations, functions, and systems to threats
- Assess the likelihood and magnitude of the resultant risks to the objectives
- Design, implement and operate controls to mitigate those risks to acceptable levels

Both sets of criteria, which are attached to this letter, were developed after careful consideration of the set of information elements best able to meet the cybersecurity information needs of a broad range of users. When developing the criteria, the AICPA:

- Considered the process and control requirements identified in existing cybersecurity frameworks[3]
- Identified best practices for cybersecurity risk management and governance
- Solicited feedback from various key stakeholders, including representatives from the public, private, non-profit and government sectors, investor community, boards of directors, registrants, cybersecurity experts, and academics, through a series of focus groups and presentations
- Followed due process procedures when exposing both sets of criteria for public comment

The AICPA regularly updates the criteria for new and emerging best practices and processes.

Specific Areas of Comment

Reporting on Material Cybersecurity Incidents on Form 8-K – The AICPA supports the SEC's proposed requirements to report cybersecurity incidents on Form 8-K. We too believe that information about material cybersecurity incidents is needed to provide timely and relevant disclosure to investors and other stakeholders, such as financial analysts, investment advisers, and portfolio managers, to enable them to assess the possible short and long-term financial and operational effects on the registrant.

The AICPA believes that material cyber incidents should be reported on a timely basis. We also recognize, however, that cybersecurity incidents vary widely; some are easier to evaluate than others. Therefore, we

[3] Specifically, information from the following standards and frameworks was considered: National Institute of Standards and Technology Framework for Improving Critical Infrastructure (NIST Cybersecurity Framework or NIST CSF); ISO/IEC 27001/27002 and related standards; US Dept. of Homeland Security requirements for annual FISMA reporting; FFIEC questionnaires; COBIT; COSO's 2013 Internal Control – Integrated Framework; HIPAA Security Rule; HITRUST CSF; PCI DSS; and NIST Special Publication 800 series

believe that registrants are likely to benefit from additional guidance in certain areas, including the following, that may prove to be particularly challenging:

- Consideration of the period of time between incident occurrence, detection, and determination of materiality, given that the length of time between each may vary because of the nature of the incident
- Determination of an incident's materiality, including the nature and extent of information needed to make that determination
- Consideration of timely reporting, including in situations in which law enforcement authorities have requested that the registrant not disclose a material incident for a period of time
- Consideration of how individual immaterial incidents should be aggregated when determining materiality, including the effect of the period over which the incidents take place, the correlation between incidents, and the effect of multiple incidents on cybersecurity risk
- Consideration of how incidents that occurred at a service provider should be evaluated as material to the registrant

As noted in Appendix A, the *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* also calls for organizations to make certain disclosures about significant cybersecurity incidents. In addition, the definition of cybersecurity incidents to be disclosed is similar to those included in the SEC's proposed disclosures. The AICPA supports the SEC's position that, when making those disclosures, registrants must weigh investors' need for incident disclosures against the risk of providing those disclosures "at such a detailed level that the likelihood of a hostile party exploiting a security vulnerability is increased."[4]

Disclosures about Cybersecurity Incidents in Periodic Reports – The AICPA also supports the proposed requirements to update information about cybersecurity incidents that was previously disclosed in quarterly filings.

Disclosures of Registrant's Risk Management, Strategy, and Governance over Cybersecurity – As cybersecurity concerns grow, investors, consumers, regulators, public advocacy groups, and other stakeholders are demanding greater transparency about how organizations of all sizes and industries manage their cybersecurity risks. Therefore, the AICPA supports the need for robust and transparent cybersecurity disclosures by registrants.

We also agree with the focus of the proposed disclosures on the registrant's risk assessment process, which is critical to establishing an effective cybersecurity risk management program. Without identifying and assessing the unique risks that may prevent a registrant from achieving its cybersecurity objectives, the registrant is unable to design effective policies and procedures to mitigate those risks. In addition, periodic reassessment of risks and control monitoring are necessary elements of an effective cybersecurity program. In addition, we agree that an effective cybersecurity risk management program must address the cybersecurity risks introduced by third parties with whom registrants do business. Therefore, we support the proposed requirement that a registrant be required to disclose the policies and procedures it has designed and

[4] *AICPA Guide: Reporting on an Entity's Cybersecurity Risk Management Program*, paragraph 3.18.

implemented to manage cybersecurity risks associated with its use of third-party service providers, particularly those policies and procedures it uses to mitigate cybersecurity risks related to those providers.

As noted in Appendix A, the AICPA believes many of the SEC's proposed disclosures around risk management, strategy, and governance align with the disclosures covered by the AICPA's *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*.

Disclosures of Cybersecurity Risks and Incidents – The AICPA also supports the Commission's proposed requirements for enhanced disclosures to investors and other stakeholders about organizations' cybersecurity risks and incidents. We believe that the proposed disclosures would provide more consistent, comparable, and reliable information for investors and additional clarity for registrants.

While we recognize that the definition of materiality included in the proposed disclosures is consistent with the definition of materiality as set forth by the Supreme Court, we believe registrants may benefit from additional guidance on how to determine whether a cyber incident is material for disclosure purposes. In addition, we believe additional clarity is needed for registrants to understand how to aggregate similar and dissimilar incidents when determining whether a material cybersecurity incident has occurred.

Disclosures Regarding the Board of Directors' Cybersecurity Expertise– The AICPA agrees that investors and other stakeholders may benefit from disclosures related to board members' cybersecurity expertise. Understanding such matters enables investors to consider the importance a registrant places in effectively managing its cybersecurity risks. As indicated in Appendix A, the AICPA's *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* also cover disclosure of "the process for board oversight of the entity's cybersecurity risk management program."

In some situations, however, board members need not be cybersecurity specialists to oversee an organization's cybersecurity efforts; instead, they need only possess sufficient knowledge and understanding of the cyber risks unique to the organization to meet their oversight responsibilities. Registrants should be free to determine the level of board cybersecurity expertise required and the best manner in which to obtain such expertise. Some boards may be able to leverage the deep cybersecurity expertise of senior executives with the organizations, while others may decide to engage independent cybersecurity experts to provide trust and credibility around the organization's cybersecurity efforts.

For some organizations, mandating board member cybersecurity expertise may inhibit recruitment of board members who possess other skills or competencies (for example, ESG) that may be more important to the organization. Such a mandate may also constrain efforts to establish a diverse board of directors who possess a different yet complementary set of skills and competencies necessary to effectively oversee the organization.

Other Matters

Need for Globally Accepted Cybersecurity Reporting and Evaluation Standards. In its recent proposed rules for climate-related disclosures, the SEC indicated its efforts to align its climate-related disclosure framework with existing global standards for climate change disclosures.[5] Similarly, the AICPA believes that a broad range

[5] SEC Release Nos. 33-11042; 34-94478, *The Enhancement and Standardization of Climate-Related Disclosures for Investors*, March 2022.

of interested parties, including regulators, investors, analysts, and others, would benefit from the adoption of globally accepted cybersecurity reporting and evaluation standards. The reporting standards could be used by registrants to make consistent and comparable cybersecurity disclosures; evaluation standards could be used to determine the effectiveness of an organization's cybersecurity risk management policies and procedures.[6]

We believe it is essential that all public, private, not-for-profit, and governmental organizations, and other interested parties work toward a global solution that would provide insight into how organizations leverage their resources to address cybersecurity risks. The AICPA believes the adoption of a globally accepted reporting and evaluation reporting framework would have the following benefits:

- Providing organizations with a common language to use when designing their cybersecurity risk management programs, preparing cybersecurity disclosures and when evaluating the effectiveness of their cybersecurity policies and procedures
- Providing decision-useful cybersecurity information in a manner that enhances consistency and comparability among organizations
- Reducing the communication and compliance burden on organizations, which often have to comply with a number of diverse cybersecurity frameworks and assessment programs)

Furthermore, the AICPA believes that its *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* provides robust standards that can be used as the basis for a globally accepted cybersecurity reporting framework (as noted previously, the Description Criteria are principles-based rather than rules-based to support the ability of organizations to meet the differing cybersecurity risk management information needs of a variety of stakeholders). Use of a global set of reporting and evaluation standards, when coupled with CPA involvement, can enhance the trust and confidence users place in cybersecurity information. For example, boards of directors and audit committees may find a CPA's report[7] helpful in meeting their oversight responsibilities.

Managing Third-Party Risks Through SOC 2 Reports. Most organizations rely on third-party service providers to perform critical business functions. To achieve their commitments to customers and others and to comply with law and regulations to which they are subject, organizations often need to obtain assurances from those third-party service providers that their systems and controls support the organization's objectives.

Because of the number of divergent cybersecurity frameworks in the market today, the cybersecurity landscape is a confusing place for organizations, stakeholders and other interested parties who want to know more about service providers' cybersecurity efforts. Now, as never before, there is a need for clarity around the types of cybersecurity disclosures that would best meet the information needs of users. As noted in the proposed disclosures around risk management and strategy, this issue can best be addressed by providing investors with consistent, comparable information about how organizations oversee and manage their cybersecurity risks, including the risks that arise from doing business with third-party service providers.

---

[6] Ideally, that same disclosure and evaluation criteria could be used by CPAs (or other independent, third-party assessors) to provide assurance on that information, if and when the market demands it.

[7] In accordance with the AICPA's attestation standards, CPAs may examine and report on whether disclosures included in a description of an organization's cybersecurity risk management program are presented in accordance with the *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program*.

Part of the AICPA's SOC suite of services, SOC 2 reports were developed to meet the needs of a broad range of users by addressing the processes and controls that affect the security, availability, and processing integrity of the systems used to process users' data, and the confidentiality and privacy of the information processed by those systems. SOC 2 reports include a robust description of the systems used by a service provider to provide services to users and, in most cases, an evaluation of the effectiveness of system controls to achieve the provider's service commitments and system requirements. They also generally include an independent CPA's opinion on whether (a) the description is presented in accordance with the AICPA's *Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* and (b) the security policies and procedures are suitably designed and operated effectively to achieve those commitments and requirements. The increased demand for SOC 2 reports over the past several years demonstrates the value that organizations place on such reports for managing a number of third-party risks, including cybersecurity, availability, and confidentiality.

Assurance – For decades, CPAs have been enhancing the confidence users have in historical financial statements through the audit process. Audited financial statements are trusted because the market understands the benefits of having an independent CPA provide an audit.

Likewise, CPAs can provide assurance on cybersecurity information by applying the AICPA's *Statements on Standards for Attestation Engagements* (SSAEs), while at the same time complying with the AICPA's *Code of Professional Conduct* and *Statements on Quality Control Standards*. These standards require CPAs to be independent, have the appropriate competence and capabilities including sufficient knowledge of the subject matter, follow supervision and review requirements, and incorporate the work of specialists, when necessary, among other requirements. In addition, work performed by CPAs is subject to quality monitoring programs (including reviews of engagements and quality management reviews) intended to enhance the quality of the work performed.

Today, many CPA firms employ both licensed CPAs and information technology and security specialists. Using a set of suitable criteria (such as the *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* and the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*), CPA firms can provide assurance on an organization's cybersecurity disclosures, and on the effectiveness of its cybersecurity controls and other activities it uses to mitigate identified cybersecurity risks. Boards of directors and audit committees may find CPAs' reports on such management-prepared information helpful in meeting their oversight responsibilities.[8]

Structured data – We agree with the SEC's proposal that cybersecurity information be provided in Inline XBRL format. Submission in this format allows for the information to be more efficiently searched, consumed, and analyzed by investors, regulators, and other stakeholders. Structuring cybersecurity information in this manner would offer users a cost-effective manner to consume this information, similarly to how they consume financial information.

[8] A CPA may examine and report on such information in accordance with the AT-C sections 105 and 205 of the AICPA's *Statements on Standards for Attestation Engagements*. A CPA's SOC for Cybersecurity examination, performed in accordance with those same standards and the AICPA guide, *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, would also result in a CPA's opinion on a description of an organization's cybersecurity risk management program as well as an opinion on the operating effectiveness of the cybersecurity controls within that program.

We appreciate the SEC taking leadership on this critical issue and would be pleased to discuss our comments or answer any questions regarding the AICPA Cybersecurity Reporting framework and the views expressed in this letter.

Respectfully,

Susan S. Coffey, CPA, CGMA

Chief Executive Officer – Public Accounting

About the AICPA

The AICPA is the world's largest member association representing the CPA profession, with more than 428,000 members in the United States and worldwide, and a history of serving the public interest since 1887. AICPA members represent many areas of practice, including business and industry, public practice, government, education, and consulting. The AICPA sets ethical standards for its members and U.S. auditing and attestation standards for private companies, not-for-profit organizations, and federal, state, and local governments. It develops and grades the Uniform CPA Examination, offers specialized credentials, builds the pipeline of future talent, and drives continuing education to advance the vitality, relevance, and quality of the profession.

APPENDIX A – Mapping of SEC's Proposed Cybersecurity Disclosures to Related Elements in the AICPA's Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program

SEC's Proposed Cybersecurity Disclosures	AICPA's Description Criteria[9]
B. Reporting of Cybersecurity Incidents on Form 8-K. **1. Overview of Proposed Item 1.05 of Form 8-K** The following disclosures on Form 8-K, within 4 days, for a material cybersecurity incident: • When the incident was discovered and whether it is ongoing. • A brief description of the nature and scope of the incident. • Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose; • The effect of the incident on the registrant's operations; and • Whether the registrant has remediated or is currently remediating the incident. • An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.	**DC6:** For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of those incidents and their disposition.
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (i) The registrant has a cybersecurity risk assessment program, and if so, provide a description of such program;	**DC2:** The principal types of sensitive information created, collected, transmitted, used, or stored by the entity
	DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing
	DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives
	DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program
	DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities
	DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes

[9] This column includes a reference to select description criteria (DC) in the AICPA's *Description Criteria for Use in the Cybersecurity Risk Management Program*. The Description Criteria, attached to this letter, contains implementation guidance for each of the referenced disclosures.

SEC's Proposed Cybersecurity Disclosures	AICPA's Description Criteria[9]
	that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives
	DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both
	DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program
	DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness key control activities and other components of internal control related to cybersecurity
	DC17: The process for developing a response to assessed risks, including the design and implementation of control processes
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (ii) The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;	**DC11:** The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (iii) The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider, including, but not limited to, those providers that have access to the registrant's customer and employee data. If so, the registrant shall describe these policies and procedures, including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other	**DC12:** The process for identifying, assessing, and managing the risks associated with vendors and business partners

SEC's Proposed Cybersecurity Disclosures	AICPA's Description Criteria[9]
mechanisms the company uses to mitigate cybersecurity risks related to these providers;	
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (iv) The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents, and if so, provide a description of the types of activities undertaken;	**DC17**: The process for developing a response to assessed risks, including the design and implementation of control processes
	DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following: a. Prevention of intentional and unintentional security events b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents c. Management of processing capacity to provide for continued operations during security, operational, and environmental events d. Detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability e. Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (v) The registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;	**DC19:** The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following: a. Prevention of intentional and unintentional security events b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents c. Management of processing capacity to provide for continued operations during security, operational, and environmental events d. Detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability e. Identification of confidential information when received or created, determination of the retention period for that information, retention of the

SEC's Proposed Cybersecurity Disclosures	AICPA's Description Criteria[9]
	information for the specified period, and destruction of the information at the end of the retention period
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (vi) Previous cybersecurity incidents informed changes in the registrant's governance, policies and procedures, or technologies;	**DC16**: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (vii) Cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the registrant's strategy, business model, results of operations, or financial condition and if so, how; and	**DC5:** Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity, (2) organizational and user characteristics, and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and in its environment.
	DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives
229.106 (Item 106) Cybersecurity **2 (b) Risk management and strategy** (1) Disclose ***in such detail as necessary*** cybersecurity identification and risk management policies and procedures. Disclosure should include, as applicable, and discussion of whether: (viii) Cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation, and if so, how	**DC11:** The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives
229.106 (Item 106) Cybersecurity **2 (c) Governance** (1) Describe board oversight (i) Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks; (ii) The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and (iii) Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.	**DC8:** The process for board oversight of the entity's cybersecurity risk management program

SEC's Proposed Cybersecurity Disclosures	AICPA's Description Criteria[9]
229.106 (Item 106) Cybersecurity **2 (c) Governance** (2) Describe management's role in assessing and managing cyber risk (i) Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise; (ii) Whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any such persons in such detail as necessary to fully describe the nature of the expertise; (iii) The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and (iv) Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.	**DC9:** Established cybersecurity accountability and reporting lines
	DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity
	DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

DC Section 200

Description Criteria for a Description of a Service Organization's System in a SOC 2® Report

Prepared by the AICPA Assurance Services Executive Committee's SOC 2® Working Group

Introduction

.01 AICPA's Assurance Services Executive Committee (ASEC), through its Trust Information Integrity Task Force's SOC 2® Guide Working Group, has developed a set of benchmarks, known as *description criteria*. These description criteria are to be used when preparing and evaluating the description of the service organization's system (description) in an examination of a service organization's controls over security, availability, processing integrity, confidentiality, and privacy (SOC 2® examination). This document presents the description criteria for use in that examination. (The AICPA's trust services criteria are not addressed in this document. [fn 1] Those criteria are used in a SOC 2® examination to evaluate whether controls stated in the description were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.)

.02 Applying the description criteria requires judgment. Therefore, in addition to the description criteria, this document also presents implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. This guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the service organization and its environment when applying the description criteria.

Applicability and Use of the Description Criteria

SOC 2® Examination

.03 The description criteria presented in this document were developed to be used in conjunction with the SOC 2® examination described in AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (guide). The SOC 2® examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements* (AICPA, *Pro-*

[fn 1] The trust services criteria were issued in *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* and are codified in TSP section 100 (AICPA, *Trust Services Criteria*). Paragraphs .25–.26 of TSP section 100 provide transition guidance related to the use of those criteria in a service auditor's report.

fessional Standards). In that examination, the CPA (known as a *service auditor*) [fn 2] expresses an opinion about the following:

a. Whether the description is presented in accordance with the description criteria

b. Whether the controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved if controls operated effectively based on the applicable trust services criteria

c. In a type 2 examination, [fn 3] whether the controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. [fn 4]

.04 A SOC 2® examination is predicated on the concept that, because service organization management is ultimately responsible for developing, implementing, and operating the service organization's system, service organization management is also responsible for developing and presenting in the SOC 2® report a description of the service organization's system. Service organization management uses the description criteria in this document when preparing the description of the service organization's system; the service auditor uses the criteria when evaluating whether the description is presented in accordance with the description criteria.

Suitability and Availability of the Description Criteria

.05 According to the attestation standards, the attributes of suitable criteria are as follows: [fn 5]

- *Relevance.* Criteria are relevant to the subject matter.

[fn 2] In the attestation standards, a CPA performing an attestation engagement ordinarily is referred to as a *practitioner.* However, the AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* uses the term *service auditor*, rather than practitioner, to refer to a CPA reporting on controls at a service organization. Therefore, this document also uses the term *service auditor*.

[fn 3] There are two types of SOC 2® examinations (type 1 and type 2), and the subject matters vary depending on which type of examination the service auditor performs. The subject matters of a type 1 examination are (*a*) the description and (*b*) the suitability of the design of the controls to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The subject matters in a type 2 examination are (*a*) the description, (*b*) the suitability of design of the controls to provide reasonable that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria, and (*c*) the operating effectiveness of controls to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

[fn 4] This term refers to the trust services criteria in TSP section 100, *2017Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), that pertain to the category or categories included within the scope of the particular examination.

[fn 5] Paragraph .A42 of AT-C section 105, *Concepts Common to All Attestation Engagements* (AICPA, *Professional Standards*).

- *Objectivity.* Criteria are free from bias.

- *Measurability.* Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.

- *Completeness.* Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect users' decisions made on the basis of that subject matter.

.06 In addition to being suitable, AT-C section 105 [fn 6] indicates that the criteria used in an attestation engagement should be available to report users. The publication of the description criteria makes the criteria available to report users. Accordingly, ASEC has concluded that the description criteria presented in this document are suitable and available for use in a SOC 2® examination.

Preparing and Evaluating the Presentation of the Description of the Service Organization's System in Accordance With the Description Criteria

.07 Service organization management is responsible for the design, implementation, and operation of controls within the system used to provide services to user entities and business partners. In a SOC 2® examination, a description of the service organization's system presented in accordance with the description criteria is designed to enable user entities, business partners, and other intended users of the SOC 2® report (known collectively as *report users*) to understand the service organization's system, including the processing and flow of data and information through and from the system. The description describes the procedures and controls the service organization has implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The description is prepared by service organization management from documentation supporting the system of internal control and system operations, as well as consideration of the policies, processes, and procedures within the system used to provide the services.

.08 A SOC 2® report is intended for use by those who have sufficient knowledge and understanding of the service organization, the services it provides, and the system used to provide those services, among other matters. As a result, when drafting the description, service organization management can assume that users have such knowledge and understanding. Furthermore, if the users do not have such knowledge and understanding, they are likely to misunderstand the content of the SOC 2® report, the assertions made by management, and the service auditor's opinion, all of which are included in the report. For that reason, management and the service auditor should agree on the intended users of the report (referred to as *specified parties*). Specified parties of a SOC 2® report may include service organization personnel, user entities of the system throughout some or all of the period, business partners subject to risks arising from interactions with the system, practitioners providing services to user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of such matters.

.09 Though the description is generally narrative in nature, there is no prescribed format for the description. Flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof may be used to supplement the narratives contained within the description.

[fn 6] Paragraph .25*b* of AT-C section 105.

.10 Additionally, the description can be organized in a variety of ways. For example, the description may be organized by components of internal control (the control environment, risk assessment process, control activities, monitoring activities, and information and communications). Alternatively, it may be organized by components of the system (infrastructure, software, people, procedures, and data) and supplemented by disclosures of the aspects of the internal control components relevant to the identification and assessment of risks that would prevent the service organization from achieving its service commitments and system requirements and the design, implementation, and operation of controls to address them.

.11 The extent of disclosures included in the description may vary depending on the size and complexity of the service organization and its activities. In addition, the description need not address every aspect of the service organization's system or the services provided by the system, particularly if certain aspects of those services are not relevant to report users or are beyond the scope of the SOC 2® examination. For example, disclosures about a service organization's processes related to billing for the services provided to user entities are unlikely to be relevant to report users. Similarly, although the description includes procedures within both manual and automated systems by which services are provided, it need not necessarily disclose every step in the process.

.12 Ordinarily, a description of a service organization's system in a SOC 2® examination is presented in accordance with the description criteria when it (*a*) describes the system that the service organization has implemented (that is, placed in operation) to provide the services, (*b*) includes information about each description criterion, to the extent it is relevant to the system being described, and (*c*) does not inadvertently or intentionally omit or distort information that is likely to be relevant to report users' decisions. Although the description should include disclosures about each description criterion, such disclosures are not intended to be made at such a detailed level that they might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the service organization's ability to achieve its service commitments and system requirements. Instead, the disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks.

.13 A description is not presented in accordance with the description criteria if it (*a*) states or implies that certain IT components exist when they do not, (*b*) states or implies that certain processes and controls have been implemented when they are not being performed, or (*c*) contains statements that cannot be objectively evaluated (for example, advertising puffery).

- **.14** In certain circumstances, additional disclosures may be necessary to supplement the description. Management's decisions about whether such additional disclosures are necessary and the service auditor's evaluation of management's decisions involve consideration of whether the disclosures may affect information that is likely to be relevant to the decisions of report users. Additional disclosures may include the following, for example:Significant interpretations made in applying the description criteria in the specific circumstances of the SOC 2® examination (for example, what constitutes a security event or incident)

- Subsequent events, depending on their nature and significance

Materiality Considerations When Preparing and Evaluating Whether the Description Is Presented in Accordance With the Description Criteria

.15 As discussed in paragraph .02, applying the description criteria requires judgment. One of those judgments involves the informational needs of report users. Most SOC 2® reports have a broad range of specified

parties. Therefore, the description is intended to meet the common informational needs of the specified parties and does not ordinarily include information about every aspect of the system that may be considered important to each individual report user. However, an understanding of the perspectives and information needs of the broad range of intended SOC 2® report users is necessary to determine whether the description is presented in accordance with the description criteria and is sufficient to meet report users' needs.

.16 When evaluating whether the description is in accordance with the description criteria, management considers whether misstatements or omissions in the description, individually or in the aggregate, could reasonably be expected to influence decisions of specified parties to the SOC 2® report. For example, in a SOC 2® examination on controls relevant to privacy, management may discover that is has failed to describe a principal service commitment involving compliance with the European Union's General Data Protection Regulation. Because such information could reasonably be expected to influence the decisions of SOC 2® report users, management may conclude that the omission of such information may affect the decisions of such users. In that case, management would amend the description by including the relevant information. [fn 7]

.17 Because the description criteria call for disclosure of primarily nonfinancial information, most descriptions will be presented in narrative form. Therefore, materiality considerations are mainly qualitative in nature and center around whether there are misstatements in information that could reasonably be expected to influence report users' decisions, including the possibility that relevant information has been omitted. Qualitative factors to be considered include the following:

- Whether the description of the service organization's system includes the significant aspects of system processing
- Whether the description is prepared at a level of detail likely to be meaningful to report users
- Whether each of the relevant description criteria in paragraph .19 has been addressed without using language that omits or distorts the information
- Whether the characteristics of the presentation are appropriate, because the description criteria allow for variations in presentation

Description Criteria for a Description of a Service Organization's System in a SOC 2® Examination and Related Implementation Guidance

.18 To be presented in accordance with the description criteria, a description ordinarily needs to disclose information about each of the requirements (criteria) presented in the left column of the following table, to the extent that the criterion is applicable to the system and the trust services categories included within the scope of the examination. (Materiality considerations are discussed in the previous section beginning at paragraph .15.)

[fn 7] If the description has been prepared to meet the informational needs of a specific subset of SOC 2® report users (and the report is restricted to those specific users), management considers whether misstatements (including omissions) may affect the decisions of that specific subset of report users.

.19 The implementation guidance in the right column of the following table presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, service organization management is advised to carefully consider the specific facts and circumstances of the service organization and the nature of the services provided when applying the description criteria in a SOC 2® examination.

Description Criteria	***Implementation Guidance***
The description contains the following information:	When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
DC 1: The types of services provided	Examples of the types of services provided by service organizations are as follows: • *Customer support.* Providing customers of user entities with online or telephonic post-sales support and service management. Examples of these services are warranty inquiries and investigating and responding to customer complaints. • *Health care claims management and processing.* Providing medical providers, employers, third-party administrators, and insured parties of employers with systems that enable medical records and related health insurance claims to be processed accurately, securely, and confidentially. • *Enterprise IT outsourcing services.* Managing, operating, and maintaining user entities' IT data centers, infrastructure, and application systems and related functions that support IT activities, such as network, production, security, change management, hardware, and environmental control activities. • *Managed security.* Managing access to networks and computing systems for user entities (for example, granting access to a system and preventing, or detecting and mitigating, system intrusion). • *Financial technology (FinTech) services.* Providing financial services companies with information technology-based transaction processing services. Examples of such transactions are loan processing, peer-to-peer lending, payment processing, crowdfunding, big data analytics, and asset management.
DC 2: The principal service commitments and system requirements	A system of internal control is evaluated using the trust services criteria within the context of the entity's ability to achieve its

Description Criteria	*Implementation Guidance*
	business objectives and sub-objectives. When a service organization provides services to user entities, its objectives and sub-objectives relate primarily to the following: *a.* The achievement of the service commitments made to user entities related to the system used to provide the services and the system requirements necessary to achieve those commitments *b.* Compliance with laws and regulations regarding the provision of the services by the system *c.* The achievement of the other objectives the service organization has for the system. These are referred to as the service organization's *service commitments* and *system requirements.* Although service organization management is responsible for designing, implementing, and operating controls to provide reasonable assurance that it achieves its system objectives, management is required to disclose in the description only its *principal* service commitments and system requirements, as discussed in the subsequent section. *Principal Service Commitments*. Disclosure of the principal service commitments and system requirements enables report users to understand the objectives that drive the operation of the system and how the applicable trust services criteria were used to evaluate whether controls were suitably designed and operated effectively. Service commitments include those made to user entities and others (such as customers of user entities), to the extent those commitments relate to the trust services category or categories addressed by the description. For example, service commitments could also include those made as part of the National Institute of Standards and Technology (NIST) risk management framework for government agencies and other parties. The service commitments a service organization makes to user entities and others are based on the needs of those entities. In identifying the service commitments to be disclosed, service organization management may begin by reviewing the commitments it made to user entities. Service commitments may be communicated to user entities in many ways, such as through contracts, service level agreements, and published policies (for example, a privacy policy). No specific form of communication is required. A service organization may make service commitments on many different aspects of the service being described, including the following:

Description Criteria	*Implementation Guidance*
	• Specification of the algorithm used in a calculation • The hours a system will be available • Published password standards • Encryption standards used to encrypt stored customer data Service commitments may also be made about one or more of the trust services categories addressed by the description. As an example, if controls over privacy are addressed by the description, a service organization may make commitments such as the following: • The organization will not process or transfer information without obtaining the data subject's consent. • The organization will provide a privacy notice to customers once every 6 months or when there is a change in the organization's business policies. • The organization will respond to access requests within 10 working days of receiving the request from its customers. Service organization management need not disclose every service commitment, but only those that are relevant to the broad range of SOC 2® report users (that is, the principal service commitments). For example, when the description addresses availability, a service organization may make the same system availability commitment to the majority of its user entities. Because information about the availability commitment common to most user entities is likely to be relevant to the broad range of SOC 2® report users, service organization management would describe that principal availability commitment in the description. In other cases, however, a service organization may make a different commitment about system availability to an individual user entity that requires greater system availability than most user entities. Service organization management ordinarily would not disclose that commitment because it is unlikely to be relevant to the broad range of SOC 2® report users. Because that service commitment is not disclosed in the description, the individual user entity understands that the evaluation of the

Description Criteria	*Implementation Guidance*
	suitability of design of controls and, in a type 2 examination, the operating effectiveness of controls was made based on the service organization's achievement of its principal service commitments and system requirements (that is, those common to the majority of user entities); therefore, the individual user entity may need to obtain additional information from the service organization regarding the achievement of its specific availability commitment. When the description addresses privacy, service organization management discloses the service commitments and system requirements identified in the service organization's privacy notice or in its privacy policy that are relevant to the system being described. When making such disclosures, it may also be helpful to report users if service organization management describes the purposes, uses, and disclosures of personal information as permitted by user entity agreements. *Principal System Requirements*. System requirements are the specifications about how the system should function to do the following: • Meet the service organization's service commitments to user entities and others (such as user entities' customers) • Meet the service organization's commitments to vendors and business partners • Comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations • Achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations. The following are examples of system requirements: • Workforce member fingerprinting and background checks established in government banking regulations • System edits that restrict the values accepted for system input, which are defined in application

Description Criteria	*Implementation Guidance*
	design documents • Maximum acceptable intervals between periodic review of workforce member logical access as documented in the security policy manual • Data definition and tagging standards, including any associated metadata requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol (SOAP) • Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA) System requirements may result from the service organization's commitments relating to one or more of the trust services categories (for example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration). The principal system requirements that need to be disclosed are those that are relevant to the trust services category or categories addressed by the description and that are likely to be relevant to the broad range of SOC 2® report users. In identifying which system requirements to disclose, service organization management may consider internal policies that are relevant to the system being described, key decisions made in the design and operation of the system, and other business requirements for the system. For example, internal requirements related to the operating margin for the services associated with the system are not relevant to the broad range of SOC 2® report users and, therefore, need not be disclosed.
DC 3: The components of the system used to provide the services, including the following: *a. Infrastructure* *b. Software* *c. People* *d. Procedures* *e. Data*	*Infrastructure.* Disclosures about the infrastructure component include matters such as the collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and related hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services. *Software.* Disclosures about the software component include matters such as the application programs, the IT system software that supports those application programs (operating sys-

Description Criteria	*Implementation Guidance*
	tems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop and laptop applications. *People.* Disclosures about the people component include the personnel involved in the governance, management, operation, security, and use of the system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers). *Procedures.* Disclosures about the automated and manual procedures implemented by the service organization primarily relate to those through which services are provided. These include, as appropriate, procedures through which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared. A process consists of a series of linked procedures designed to accomplish a particular goal (for example, the process for managing third party risks). Procedures are the specific actions undertaken to implement a process (for example, the procedure in place to assess and manage the requisition and engagement of vendors). For that reason, service organization management may find it easier to describe procedures in the context of the process of which they are a part. Policies are management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. The service organization deploys control activities through policies that establish what is expected and procedures that put policies into action. Reports and other information prepared by the service organization may also be included in the description to enable report users to better understand the order of activities performed by the service organization. System components may also be described using specific technical terms that will help create a clearer understanding of the service organization's system and system boundaries. Technical terms can also aid report users in understanding the service organization's physical and logical components when considering a service organization's impact on the user entities. It may be helpful for service organizations to enhance their system descriptions using open systems interconnect (OSI) seven-layer model concepts. An organization could describe how and on which layer specific components of the system are operated,

Description Criteria	*Implementation Guidance*
	for example, with a statement such as this: Encrypted connections are made to the service organization using client virtual private network (VPN) hardware that connects system users via secure shell (SSH) to secure file transfer protocol (SFTP) servers that operate following transport layer security (TLS) standards and protocols. *Data.* Disclosures about the data component include types of data used by the system, transaction streams, files, databases, tables, and output used or processed by the system. When the description addresses the confidentiality or privacy categories, other matters that may be considered for disclosure about the data component include the following: • The principal types of data created, collected, processed, transmitted, used, or stored by the service organization and the methods used to collect, retain, disclose, dispose of, or anonymize the data • Personal information that warrants security, data protection, or breach disclosures based on laws or commitments (for example, personally identifiable information, protected health information, and payment card data) • Third-party entity information (for example, information subject to confidentiality requirements in contracts) that warrants security, data protection, or breach disclosures based on laws or commitments When the description addresses controls over confidentiality and privacy, management would address, at a minimum, all the system components as they relate to the information life cycle of the confidential and personal information used in providing the service within well-defined processes and informal ad hoc procedures. *Boundaries of the system.* Not all activities performed at the service organization are part of the system being described. Determining the functions or processes that are outside the boundaries of the system and describing them in the description may be necessary to prevent report users from misunderstanding the boundaries of the system. Therefore, if there is a risk that report users might be confused about whether a specific function or

Description Criteria	*Implementation Guidance*
	process is part of the system being described, the description needs to clarify which processes or functions are included in the examination. For example, the following functions or processes at the service organization may be outside the boundaries of the system being described: • The process used to invoice user entities for the services provided by the service organization. • The conversion of new user entities to the service organization's systems. For some service organizations, such conversions are handled by an entirely different system than the one being described. • The receipt of data from sources outside the system being described. An example is a payroll processing system that receives information inputs from an employer in a ready-to-process state, which limits the responsibility of the service organization's system to processing the inputs provided by the employer to produce direct bank deposits to specified bank accounts. *Third Party Access.* Vendors, business partners, and others (third parties) often store, process, and transmit sensitive data or otherwise access a service organization's system. These third parties may provide components of the system. Service organization management may need to describe the components of the system provided by such third parties. Such disclosures may include, for example, the nature of the third parties' access and connectivity to the service organization's system.
DC 4: 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, as of the date of the description (for a type 1) or during the period of time covered by the description (for a type 2), as applicable, the following information:	Judgment is needed when determining whether to disclose an incident. However, consideration of the following matters as they relate to the system being described may help make that determination: • Whether the incident resulted from one or more controls that were not suitably designed or operating effectively • Whether the incident resulted in a significant failure in the achievement of one or more of the service organization's service commitments and system requirements

Description Criteria	*Implementation Guidance*
a. Nature of each incident *b.* Timing surrounding the incident *c.* Extent (or effect) of the incident and its disposition	• Whether public disclosure of the incident was required (or is likely to be required) by cybersecurity laws or regulations • Whether the incident had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing • Whether the incident resulted in sanctions by any legal or regulatory agency • Whether the incident resulted in the service organization's withdrawal from material markets or cancellation of material contracts Disclosures about identified security incidents are not intended to be made at a detailed level, which might increase the likelihood that a hostile party could exploit a security vulnerability, thereby compromising the service organization's ability to achieve its service commitments and system requirements. Rather, the disclosures are intended to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks. Assume that the service organization identified a security breach that resulted in the service organization's failure to achieve one or more of its service commitments and system requirements. The breach, which occurred six months prior to the start of the period covered by the description, had not been fully remediated during the period covered by the description. In this example, management would likely need to disclose the incident in the description to enable report users to understand the nature of the risks faced by the service organization and the impact of the realization of those risks. In addition, service organization management should consider whether to disclose known incidents at a subservice organization, regardless of whether management has elected to use the inclusive or carve-out method.
DC 5: The applicable trust services criteria and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), presents the criteria for each of the trust services categories. A description is presented in accordance with this criterion when it includes information about each of the criteria related to the trust services category or categories covered by the description (applicable trust services criteria), including controls related to the control environment, risk assessment process, information and communica-

Description Criteria	*Implementation Guidance*
	tion, monitoring activities, and control activities. For example, if the description addresses availability, management would provide information about the controls it has implemented to address the common criteria in the trust services criteria and the additional trust services criteria for availability.
DC 6: If service organization management assumed, in the design of the service organization's system, that certain controls would be implemented by user entities, and those controls are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved, those complementary user entity controls (CUECs)	*Complementary User Entity Controls.* CUECs are those controls that service organization management assumed, in the design of the system, would be implemented by user entities and are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Usually, a service organization can achieve its service commitments and system requirements without depending on the implementation of CUECs at user entities because the service organization restricts its service commitments and system requirements to those matters that are its responsibility and that it can reasonably perform. Consider trust services criterion (CC) 6.2: > Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. CC 6.2 limits the service organization's responsibilities because the criterion requires only that the system register a user (identified by the user entity as an authorized user) and issue system credentials to that user after the user entity supplies the service organization with a list of authorized users. The user entity is responsible for identifying the users and supplying the service organization with a list of authorized users. If the user entity provides a list that inadvertently includes employees who are not authorized, the service organization has still met the criterion. Accordingly, identifying the authorized users and communicating that information to the service organization are not considered CUECs. The description is presented in accordance with this criterion if the CUECs are complete, accurately described, and relevant to the service organization's achievement of its service commitments and system requirements. *User Entity Responsibilities.* In addition to CUECs, user entities may have other responsibilities when using the system. Those responsibilities are necessary for the user entity to derive

Description Criteria	*Implementation Guidance*
	the intended benefits of using the services of the service organization. For example, the user of an express delivery service is responsible for providing complete and accurate recipient information and for using appropriate packaging materials. Such responsibilities are referred to as user entity responsibilities. Trust services criterion CC 2.3 states *[t]he entity communicates with external parties regarding matters affecting the functioning of internal control*. This would include communication of user responsibilities. However, because user entity responsibilities can be voluminous, they are often communicated through other methods (for example, by describing them in user manuals). Consequently, disclosure of user entity responsibilities in the description is usually not practical. Instead, management ordinarily identifies in the description the types of communications it makes to external users about user entity responsibilities. The form and content of such communication is the responsibility of service organization management. When service organization management communicates user entity responsibilities only to specific parties (such as in contracts with user entities), management considers whether other intended users of the SOC 2® report are likely to misunderstand it; in that case, management should limit the use of the report to those specific parties. If service organization management does not want to limit the use of the report, management would include the significant user entity responsibilities in the description of the service organization's system to prevent users from misunderstanding the system and the service auditor's report. In that case, the report would be appropriate for the broad range of SOC 2® users. When service organization management includes significant user entity responsibilities in the description, management evaluates those disclosures as part of its evaluation about whether the description is presented in accordance with the description criteria.
DC 7: If 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, the following: *a.* When service or-	*Inclusive method.* When service organization management elects the inclusive method, the relevant aspects of the subservice organization's infrastructure, software, people, procedures and data are considered part of the service organization's system and are included in the description of the service organization's system. Although the relevant aspects are considered a part of the service organization's system, the portions of the system that are attributable to the subservice organization would be separately identified in the description. Such disclosures include the aspects of the internal control components relevant to identification and assessment of risks that would prevent the service organization from achieving its service

Description Criteria	*Implementation Guidance*
ganization management elects to use the inclusive method: i. The nature of the service provided by the subservice organization ii. The controls at the subservice organization that 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 iii. Relevant aspects of the subservice organization's infrastructure, software, people, procedures, and data iv. The portions of the sys-	commitments and system requirements and the design, implementation, and operation of controls to address them. The description would separately identify controls at the service organization and controls at the subservice organization. However, there is no prescribed format for differentiating between the two. *Carve-out method.* When service organization management elects the carve-out method, consideration may be given to disclosure of the identity of the subservice organization when such information may be useful to user entities or business partners who want to obtain information about and perform procedures related to the services provided by the subservice organization. Complementary subservice organization controls (CSOCs) are controls that service organization management assumed, in the design of the system, would be implemented by subservice organizations and are necessary, in combination with controls at the service organization to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. When using the carve-out method, the description would identify the types of CSOCs that the subservice organization is assumed to have implemented. It is important that the description also includes the subservice organization's responsibilities for implementing those CSOCs and indicates that the related service commitments and system requirements can be achieved only if the CSOCs are suitably designed and operating effectively during the period addressed by the description. To be meaningful to report users, management includes only CSOCs that are specific to the services provided by the system being described. CSOCs may be presented as broad categories of controls or as control objectives rather than as individual controls. Service organization management may wish to include in the description a table that identifies those instances in which service commitments and system requirements are achieved solely by the service organization's controls and those in which a combination of controls at the service organization and CSOCs are needed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. Examples of CSOCs include the following: • Controls relevant to the completeness and accuracy of transaction processing on behalf of the

Description Criteria	*Implementation Guidance*
tem that are attributable to the subservice organization *b.* When service organization management decides to use the carve-out method: i. The nature of the service provided by the subservice organization ii. Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization iii. The types of controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that are necessary, in	service organization • Controls relevant to the completeness and accuracy of specified reports provided to and used by the service organization • General IT controls relevant to the processing performed for the service organization • Data centers are protected against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). The description is presented in accordance with this criterion if the CSOCs are complete, accurately described, and relevant to the service organization's achievement of the service commitments and system requirements related to the system being described. *Other matters.* A service organization that uses multiple subservice organizations may prepare its description using the carve-out method for one or more subservice organizations and the inclusive method for others. Regardless of the method service organization management selects, the description needs to disclose controls designed to provide reasonable assurance that the service organization's service commitments and system requirements are achieved, which include controls that the service organization uses to monitor the services provided by the subservice organization. Such monitoring controls may include, but are not limited to, a combination of the following: • Testing of controls at the subservice organization by members of the service organization's internal audit function • Reviewing and reconciling output reports • Holding periodic discussions with the subservice organization personnel and evaluating subservice organization performance against established service level objectives and agreements • Making site visits to the subservice organization • Inspecting type 2 SOC 2® reports on the subservice organization's system

Description Criteria	*Implementation Guidance*
combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved (commonly referred to as complementary subservice organization controls or CSOCs)	• Monitoring external communications, such as complaints from user entities relevant to the services performed by the subservice organization
DC 8: Any specific criterion of the applicable trust services criteria that is not relevant to the system and the reasons it is not relevant	If one or more applicable trust services criteria are not relevant to the system being described, service organization management includes in the description an explanation of why such criteria are not relevant. For example, an applicable trust services criterion may not be relevant if it does not apply to the services provided by the service organization. Assume user entities—not the service organization—collect personal information from the user entities' customers. When the description addresses controls over privacy, service organization management would not disclose in its description the user entities' controls over collection; however, the reason for that omission would be disclosed. In contrast, the existence of a policy prohibiting certain activities is not sufficient to render a criterion not applicable. For example, when the description addresses controls over privacy, it would be inappropriate for service organization management to omit from the description disclosures of personal information to third parties based only on the fact that the service organization's policies forbid such disclosures. Instead, the description would describe the policies and related controls for preventing or detecting such disclosures.

Description Criteria	*Implementation Guidance*
DC 9: In a description that covers a period of time (type 2 examination), the 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	Significant changes to be disclosed consist of those that are likely to be relevant to the broad range of report users. Disclosure of such changes is expected to include an appropriate level of detail, such as the date the changes occurred and how the system differed before and after the changes. Examples of significant changes to a system include the following: • Changes to the services provided • Significant changes to IT and security personnel • Significant changes to system processes, IT architecture and applications, and the processes and system used by subservice organizations • Changes to legal and regulatory requirements that could affect system requirements • Changes to organizational structure resulting in a change to internal control over the system (for example, a change to the legal entity)

Transition Guidance

.20 The description criteria presented in this document (2018 description criteria) have been designed to be used in conjunction with the use of the 2017 trust services criteria set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in a SOC 2® report. The 2018 description criteria will be codified as DC section 200 in AICPA, *Description Criteria*. The description criteria included in paragraphs 1.26–.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (2015 description criteria) will be codified as DC section 200A.

.21 When preparing a description of the service organization's system as of December 15, 2018, or prior to that date (type 1 examination) or a description for periods ending as of December 15, 2018, or prior to that date (type 2 examination), either the 2018 description criteria or the 2015 description criteria may be used. (To ensure that the 2015 description criteria are available to report users, such criteria will remain in DC section 200A through December 31, 2019.) During this transition period, management should identify in the description whether the 2018 description criteria or the 2015 description criteria were used.

.22 When preparing a description of the service organization's system as of or after December 16, 2018, (type 1 examination) or a description of the system for periods ending as of or after that date (type 2 examination), the 2018 description criteria should be used.

Appendix — Glossary

.23

For purposes of this document, the following terms have the meanings attributed as follows:

applicable trust services criteria. The criteria codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, and TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), used to evaluate controls relevant to the trust services category or categories included within the scope of a particular examination.

board or board of directors. Individuals with responsibility for overseeing the strategic direction of the service organization and the obligations related to the accountability of the service organization. Depending on the nature of the service organization, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit service organization, a board of governors or commissioners for a government service organization, general partners for a partnership, or an owner for a small business.

boundaries of the system (or system boundaries). The boundaries of a system are the specific aspects of a service organization's infrastructure, software, people, procedures, and data necessary to provide its services. When systems for multiple services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each system will differ. In a SOC 2® engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

business partner. An individual or business (and its employees), other than a vendor, who has some degree of involvement with the service organization's business dealings or agrees to cooperate, to any degree, with the service organization (for example, a computer manufacturer who works with another company who supplies it with parts).

carve-out method. Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system used to provide the services to the service organization are excluded from the description of the service organization's system and from the scope of the examination. However, the description identifies (1) the nature of the services performed by the subservice organization; (2) the types of controls expected to be performed at the subservice organization that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved; and (3) the controls at the service organization used to monitor the effectiveness of the subservice organization's controls.

complementary subservice organization controls. Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization that 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.

complementary user entity controls. Controls that service organization management assumed, in the design of the service organization's system, would be implemented by user entities and are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved.

controls at a service organization. The policies and procedures at a service organization that are part of the service organization's system of internal control. Controls exist within each of the five COSO internal control components: control environment, risk assessment, control activities, information and communication, and monitoring. The objective of a service organization's system of internal control is to provide reasonable assurance that its service commitments and system requirements are achieved.

controls at a subservice organization. The policies and procedures at a subservice organization that are relevant to the service organization's achievement of its service commitments and system requirements.

criteria. The benchmarks used to measure or evaluate the subject matter.

external users. Users, other than entity personnel, who are authorized by entity management, customers, or other authorized persons to interact with the entity's information system.

inclusive method. Method of addressing the services provided by a subservice organization in which the description of the service organization's system includes a description of the (*a*) the nature of the services provided by the subservice organization and (*b*) the components of the subservice organization's system used to provide services to the service organization, including the subservice organization's controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved. (When using the inclusive method, controls at the subservice organization are subject to the service auditor's examination procedures. Because the subservice organization's system components are included in the description, those components are included in the scope of the examination.)

information life cycle. The collection, use, retention, disclosure, disposal, or anonymization of confidential or personal information within well-defined processes and informal ad hoc procedures.

intended users. Individuals or entities that the service organization intends will be report users.

internal control. A process, effected by a service organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

operating effectiveness (or controls that are operating effectively). Controls that operated effectively provide reasonable assurance of achieving the service organization's service commitments and system requirements based on the applicable trust services criteria.

personal information. Information that is about, or can be related to, an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

privacy notice. A written communication by entities that collect personal information to the individuals about whom personal information is collected that explains the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

report users (specified users or specified parties) of a SOC 2® report. In this document, the term refers to users of a SOC 2® report. The service auditor's report included in a SOC 2® report ordinarily includes an alert restricting the use of the report to specified parties who possess sufficient knowledge and understanding of the service organization and the system to understand the report. The expected knowledge is likely to include an understanding of the following matters:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

Users likely to possess such knowledge include user entities and their personnel, business partners and their personnel, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who understand how the service organization's system may be used to provide the services.

service auditor. As used in this document, a CPA who performs a SOC 2® examination of controls within a service organization's system relevant to security, availability, processing integrity, confidentiality, or privacy.

service commitments. Declarations made by service organization management to user entities and others (such as user entities' customers) about the system used to provide the service. Service

commitments can be communicated in written individualized agreements, standardized contracts, service-level agreements, or published statements (for example, in a security practices statement).

service organization. An organization, or segment of an organization, that provides services to user entities.

SOC 2® examination. An examination engagement to report on whether (*a*) the description of the service organization's system is in accordance with the description criteria, (*b*) the controls were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and (*c*) in a type 2 report, the controls operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The SOC 2® examination is performed in accordance with the attestation standards and the AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

subsequent events. Events or transactions that occur after the specified period covered by the engagement, but prior to the date of the service auditor's report, which could have a significant effect on the evaluation of the presentation of the description of the service organization's system or the evaluation of the suitability of design and operating effectiveness of controls.

subservice organization. A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

suitability of design (or suitably designed controls). Controls are suitably designed if they have the potential to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved. Suitably designed controls are operated as designed by persons who have the necessary authority and competence to perform the control.

system. Refers to the infrastructure, software, procedures, and data that are designed, implemented, and operated by people to achieve one or more of the organization's specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

system components. Refers to the individual elements of a system, which may be classified into the following five categories: infrastructure, software, people, procedures, and data.

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in a service organization's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems, (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data, or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of service organization management to prevent or reduce the impact of the event on the service organization's achievement of its service commitments and system requirements.

system requirements. Specifications about how the system should function to (*a*) meet the service organization's service commitments to user entities and others (such as user entities' customers); (*b*) meet the service organization's commitments to vendors and business partners; (*c*) to comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other objectives of the service organization that are relevant to the trust services categories addressed by the description. Requirements are often specified in the service organization's system policies and procedures, system design documentation, contracts with customers, and government regulations.

user entity. An entity that uses the services provided by a service organization.

vendor. An individual or business (and its employees) engaged to provide services to the service organization. Depending on the services a vendor provides (for example, if it operates certain controls on behalf of the service organization that are necessary, in combination with the service organization's controls, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved), a vendor might also be a subservice organization.

AICPA

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Includes March 2020 updates

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

(This version includes revisions made in March 2020, as discussed in the Notice to Readers.)

Notice to Readers

The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* presents control criteria established by the Assurance Services Executive Committee (ASEC) of the AICPA for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems (*a*) across an entire entity; (*b*) at a subsidiary, division, or operating unit level; (*c*) within a function relevant to the entity's operational, reporting, or compliance objectives; or (*d*) for a particular type of information used by the entity.

In developing and establishing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*, [fn 1] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. Paragraph .A44 of AT-C section 105, *Concepts Common to All Attestation Engagements*, [fn 2] indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable.

This version of the trust services criteria has been modified by AICPA staff to include conforming changes necessary because of the issuance, in March 2020, of a new SOC examination. In a SOC for Supply Chain examination, a practitioner examines and reports on the effectiveness of controls (suitability of design and operating effectiveness) relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of information processed by a system that produces, manufactures, or distributes products.

These changes, which have been reviewed by the ASEC chair, were made to provide greater flexibility for use of the trust services criteria in a SOC for Supply Chain examination. It is important to note that these changes do not alter in any way the trust services criteria used to evaluate controls in a SOC 2®, SOC 3®, or SOC for Cybersecurity examination.

[fn 1] All BL sections can be found in AICPA *Professional Standards*.

[fn 2] All AT-C sections can be found in AICPA *Professional Standards*.

For users who want to see all conforming changes made to this version of the trust services criteria, a red-lined version is available at https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria-redline-2019.pdf.

Background

.01 The AICPA Assurance Services Executive Committee (ASEC) has developed a set of criteria (trust services criteria) to be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity, a division, or an operating unit of an entity. In addition, the trust services criteria may be used when evaluating the design and operating effectiveness of controls relevant to the security, availability, processing integrity, confidentiality or privacy of a particular type of information processed by one or more of an entity's systems or one or more systems used to support a particular function within the entity. This document presents the trust services criteria.

.02 As in any system of internal control, an entity faces risks that threaten its ability to achieve its objectives based on the trust services criteria. Such risks arise because of factors such as the following:

- The nature of the entity's operations
- The environment in which it operates
- The types of information generated, used, or stored by the entity
- The types of commitments made to customers and other third parties
- Responsibilities entailed in operating and maintaining the entity's systems and processes
- The technologies, connection types, and delivery channels used by the entity
- The use of third parties (such as service providers and suppliers), who have access to the entity's system, to provide the entity with critical raw materials or components or operate controls that are necessary, in combination with the entity's controls, to achieve the system's objectives
- Changes to the following:
    - — System operations and related controls
    - — Processing volume
    - — Key management personnel of a business unit, supporting IT, or related personnel
    - — Legal and regulatory requirements with which the entity needs to comply
- Introduction of new services, products, or technologies

An entity addresses these risks through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance of achieving the entity's objectives.

.03 Applying the trust services criteria in actual situations requires judgment. Therefore, in addition to the trust services criteria, this document presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its *Internal Control — Integrated Framework* (the COSO framework), [fn 3] states that points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus in this document may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both management and the practitioner when they are evaluating whether the controls were suitably designed and operated effectively to achieve the entity's objectives based on the trust services criteria.

.04 Some points of focus may not be suitable or relevant to the entity or to the engagement to be performed. In such situations, management may customize a particular point of focus or identify and consider other characteristics based on the specific circumstances of the entity. Use of the trust services criteria does not require an assessment of whether each point of focus is addressed. Users are advised to consider the facts and circumstances of the entity and its environment in actual situations when applying the trust services criteria.

Organization of the Trust Services Criteria

.05 The trust services criteria presented in this document have been aligned to the 17 criteria (known as *principles*) presented in the COSO framework, which was revised in 2013. In addition to the 17 principles, the trust services criteria include additional criteria supplementing COSO principle 12: *The entity deploys control activities through policies that establish what is expected and procedures that put policies into action* (supplemental criteria). The supplemental criteria, which apply to the achievement of the entity's objectives relevant to a trust services engagement, are organized as follows:

- *Logical and physical access controls.* The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access
- *System operations.* The criteria relevant to how an entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations
- *Change management.* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made
- *Risk mitigation.* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners

.06 In addition to the 17 principles in the COSO framework, certain of the supplemental criteria are shared amongst all the trust services categories (see the section "Trust Services Categories"). For example, the

---

[fn 3]

criteria related to logical access apply to the security, availability, processing integrity, confidentiality, and privacy categories. As a result, the trust services criteria consist of

- criteria common to all five of the trust services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

.07 The common criteria provide specific criteria for addressing the following:

- The control environment (CC1 series)
- Communication and information (CC2 series)
- Risk assessment (CC3 series)
- Monitoring of controls (CC4 series)
- Control activities related to the design and implementation of controls (CC5 series)

The common criteria are suitable for evaluating the effectiveness of controls to achieve an entity's system objectives related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific trust services category or categories addressed by the engagement. The criteria for each trust services category addressed by the engagement are considered complete only if all the criteria associated with that category are addressed by the engagement.

Trust Services Category	***Common Criteria***	***Additional Category-Specific Criteria***
Security	X	N/A
Availability	X	X (A series)
Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

.08 The practitioner may report on any of the trust services categories of security, availability, processing integrity, confidentiality, or privacy, either individually or in combination with one or more of the other trust services categories. For each category addressed by the engagement, all criteria for that category are usually addressed. However, in limited circumstances, such as when the scope of the engagement is to report on a system and a particular criterion is not relevant to the services provided by a service organization, one or more criteria may not be applicable to the engagement. For example, when reporting on

privacy for a service organization's system, criterion P3.1, *Personal information is collected consistent with the entity's objectives related to privacy*, is not applicable for a service organization that does not directly collect personal information from data subjects.

Trust Services Categories

.09 The table in paragraph .24 presents the trust services criteria and the related points of focus. In that table, the trust services criteria are classified into the following categories:

a. *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 or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

b. *Availability.* Information and systems are available for operation and use to meet the entity's objectives.

Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

c. *Processing integrity (over the provision of services or the production, manufacturing, or distribution of goods).* System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity. In a SOC for Supply Chain examination, processing integrity refers to whether processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the products' specifications.

d. *Confidentiality.* Information designated as confidential is protected to meet the entity's objectives.

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

e. *Privacy.* Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Although confidentiality applies to various types of sensitive information, *privacy* applies only to personal information.

The privacy criteria are organized as follows:

i. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.

ii. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

iii. *Collection.* The entity collects personal information to meet its objectives related to privacy.

iv. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.

v. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

vi. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

vii. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.

viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

.10 As previously stated, the trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories (security, availability, processing integrity, confidentiality, or privacy), either individually or in combination with controls in other categories.

Application and Use of the Trust Services Criteria

.11 The trust services criteria were designed to provide flexibility in application and use for a variety of different subject matters. The following are the types of subject matters a practitioner may be engaged to report on using the trust services criteria:

- The effectiveness of controls within an entity's cybersecurity risk management program to achieve the entity's cybersecurity objectives using the trust services criteria relevant to security, availability, and confidentiality as *control criteria* in a SOC for Cybersecurity examination. [fn 4]

- The suitability of design and operating effectiveness of controls included in management's description of a service organization's system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, or privacy throughout a specified period to achieve the entity's objectives based on those criteria in a type 2 SOC 2 engagement. A type 2 SOC 2 engagement, which includes an opinion on the operating effectiveness of controls, also includes a detailed description of tests of controls performed by the service auditor and the results of those tests. A type 1 SOC 2 engagement addresses the same subject matter as a type 2 SOC 2 engagement; however, a type 1 SOC 2 report does not contain an opinion on the operating effectiveness of controls nor a detailed description of tests of controls performed by the service auditor and the results of those tests. [fn 5]

- The design and operating effectiveness of a service organization's controls over a system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, and privacy in a SOC 3 engagement. A SOC 3 report contains an opinion on the operating effectiveness of controls but does not include a detailed description of tests of controls performed by the service auditor and the results of those tests.

[fn 4] AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* (the cybersecurity guide) provides practitioners with performance and reporting guidance for a SOC for Cybersecurity examination.

[fn 5] AICPA Guide *SOC 2® Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, issued in 2018, contains performance and reporting guidance for SOC 2 examinations.

- The suitability of design and operating effectiveness of controls of an entity, other than a service organization, over one or more systems relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality, or privacy (for example, a SOC for Supply Chain examination).

- The suitability of the design of an entity's controls over security, availability, processing integrity, confidentiality, or privacy to achieve the entity's objectives based on the related trust services criteria. [fn 6]

.12 Practitioners generally do not use the trust services criteria when engaged to report on an entity's compliance, or on an entity's internal control over compliance with laws, regulations, rules, contracts, or grant agreements. If the practitioner is engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements in connection with an examination of the design and operating effectiveness of an entity's controls (for example, in a privacy engagement performed in accordance with AT-C section 105 and AT- Csection 205, *Examination Engagements*), the compliance portion of the engagement would be performed in accordance with AT-C section 105 and AT-C section 315, *Compliance Attestation*.

.13 Many of the trust services criteria include the phrase *to meet the entity's objectives.* Because the trust services criteria may be used to evaluate controls relevant to a variety of different subject matters (see paragraph .11) in a variety of different types of engagements (see paragraphs .20–.23), interpretation of that phrase depends upon the specific circumstances of the engagement. Therefore, when using the trust services criteria, consideration is given to how the *entity's objectives* referred to in the criteria are affected by the subject matter and scope of the particular engagement.

.14 For example, consider the following engagements:

- In a SOC 2 engagement to examine and report on a service organization's controls over the security, availability, processing integrity, confidentiality, or privacy of a *system*, management is responsible for meeting its commitments to customers. Therefore, the *objectives* in a SOC 2 engagement relate *to meeting its commitments to customers and system requirements. Commitments* are the declarations made by management to customers regarding the performance of one or more of the entity's systems. Such commitments generally are included in written contracts, service level agreements, or public statements (for example, a privacy notice). Some commitments are applicable to all customers (baseline commitments), whereas others are designed to meet individual customer needs and result in the implementation of processes or controls, in addition to those required to meet the baseline commitments. *System requirements* refer to how the system should function to achieve the entity's commitments to customers, relevant laws and regulations, or guidelines of industry groups, such as trade or business associations.

[fn 6] AT-C section 9205, *Examination Engagements: Attestation Interpretations of Section 205*, addresses an engagement such as this in Interpretation No. 2, "Reporting on the Design of Internal Control" (AT-C sec. 9205 par. .04–.14). That document states that a practitioner may examine the suitability of the design of controls under AT-C section 205, *Examination Engagements*. Paragraph .10 of AT-C section 205 provides guidance on how a practitioner should report when the engagement is over controls that have not yet been implemented.

- In a SOC for Supply Chain engagement to examine and report on an entity's controls over the security, availability, processing integrity, confidentiality, or privacy of a system used to produce, manufacture, or distribute products, management is responsible for establishing principal system objectives. Such objectives are embodied in the product commitments the entity makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. Commitments may also relate to other matters (for example, conforming with a variety of other standards and criteria such as the risk entity management framework issued by the National Institute of Standards and Technology, the cybersecurity standards issued by the International Organization for Standardization [ISO], or the Food and Drug Administration regulations on electronic records and electronic signatures included in Code of Federal Regulations, *Electronic Records; Electronic Signatures*, Title 21, Part 11).

- In an entity-wide SOC for Cybersecurity examination, the entity establishes *cybersecurity objectives. Cybersecurity objectives* are those that could be affected by cybersecurity risk and, therefore, affect the achievement of the entity's compliance, reporting, and operational objectives. The nature of an entity's cybersecurity objectives will vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, and other factors. For example, a telecommunication entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an online dating entity is likely to regard the privacy of the personal information collected from customers to be a critical factor in achieving its operating objectives. [fn 7]

.15 As an example of how the different subject matters and engagement scopes affect the use of the trust services criteria, consider trust services criterion CC6.4:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

.16 In the SOC 2 engagement example discussed in paragraph .14, the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel *to meet the service organization's commitments and system requirements.*

.17 In addition, criterion CC6.4 would only be applied as it relates to controls over the trust services category(ies) relevant to the system(s) included within the scope of the SOC 2 engagement.

[fn 7] The practitioner's responsibility is similar to that in AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, which requires the service auditor in a SOC 1® engagement to determine whether the control objectives stated in management's description of the service organization's system are reasonable in the circumstances.

.18 In the SOC for Cybersecurity examination example in paragraph .14, the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's cybersecurity objectives.

.19 In addition, criterion CC6.4 would be applied as it relates to controls within the cybersecurity risk management program (*a*) across an entire entity; (*b*) at a subsidiary, division, or operating unit level; (*c*) within a function relevant to the entity's operations, reporting, or compliance objectives; or (*d*) for a particular type of information used by the entity, depending on the scope of the SOC for Cybersecurity examination.

Professional Standards Governing Engagements Using the Trust Services Criteria

Attestation Engagements

.20 Examination engagements and engagements to apply agreed-upon procedures performed in accordance with the AICPA Statements on Standards for Attestation Engagements [fn 8] (SSAEs or attestation standards) may use the trust services criteria as the evaluation criteria. The attestation standards provide guidance on performing and reporting in connection with an examination, review, [fn 9] and agreed-upon procedures engagements. Under the attestation standards, the CPA performing an attestation engagement is known as a *practitioner*. In an examination engagement, the practitioner provides a report in which he or she expresses an opinion on subject matter or an assertion about the subject matter in relation to an identified set of criteria. In an agreed-upon procedures engagement, the practitioner does not express an opinion but, rather, performs procedures agreed upon by the specified parties and reports the results of those procedures. Examination engagements are performed in accordance with AT-C sections 105 and 205; agreed-upon procedures engagements are performed in accordance with AT-C section 105 and AT-C section 215, *Agreed-Upon Procedures Engagements*.

.21 According to the attestation standards, the criteria used in an attestation engagement should be suitable and available to report users. Attributes of suitable criteria are as follows: [fn 10]

[fn 8] Statement on Standards for Attestation Engagements No. 18, *Attestation Standards: Clarification and Recodification*, is effective for practitioners' reports dated on or after May 1, 2017.

[fn 9] Paragraph .07 of AT-C section 305, *Prospective Financial Information*, prohibits a practitioner from performing a review of internal control; therefore, practitioners may not perform a review engagement in accordance with the attestation standards using the trust services criteria.

[fn 10] Paragraph .25*b* of AT-C section 105, *Concepts Common to All Attestation Engagements*.

- *Relevance*. Criteria are relevant to the subject matter.
- *Objectivity*. Criteria are free from bias.
- *Measurability*. Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*. Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter.

.22 In addition to being suitable, AT-C section 105 indicates that the criteria used in an attestation engagement must be available to users. The publication of the trust services criteria makes the criteria available to report users. Accordingly, ASEC has concluded that the trust services criteria are suitable criteria in accordance with the attestation standards.

Consulting Engagements

.23 Sometimes, the trust services criteria may be used in engagements that involve the performance of readiness services, in which a practitioner may assist management with the implementation of one or more new information systems within an organization. [fn 11] Such engagements typically are performed under the consulting standards. In a consulting engagement, the practitioner develops findings and makes recommendations for the consideration and use of management; the practitioner does not form a conclusion about or express an opinion on the subject matter of the engagement. Generally, consulting services are performed only for the use and benefit of the client. Practitioners providing such services follow CS section 100, *Consulting Services: Definitions and Standards*. [fn 12]

Trust Services Criteria

.24 The following table presents the trust services criteria and the related points of focus. In the table, criteria and related points of focus that come directly from the COSO framework are presented using a normal font. In contrast, supplemental criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics*. Finally, criteria and points of focus that apply only when engagements using the trust services criteria are performed at a system level are presented in ***bold italics***.

[fn 11] When a practitioner provides information systems design, implementation, or integration services to an attest client, threats to the practitioner's independence may exist. The "Information Systems Design, Implementation, or Integration" interpretation (ET sec. 1.295.145) of the AICPA Code of Professional Conduct, provides guidance to practitioners on evaluating the effect of such threats to their independence.

All ET sections can be found in AICPA *Professional Standards*.

[fn 12] All CS sections can be found in AICPA *Professional Standards*.

	CONTROL ENVIRONMENT
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Sets the Tone at the Top — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
	• Establishes Standards of Conduct — The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.
	• Evaluates Adherence to Standards of Conduct — Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
	• Addresses Deviations in a Timely Manner — Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Contractors and Vendor Employees in Demonstrating Its Commitment — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.*
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

	• Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
	• Applies Relevant Expertise — The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
	• Operates Independently — The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Supplements Board Expertise — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.*
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers All Structures of the Entity — Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
	• Establishes Reporting Lines — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
	• Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.

	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Addresses Specific Requirements When Defining Authorities and Responsibilities — Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*
	• *Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities — Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.*
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Policies and Practices — Policies and practices reflect expectations of competence necessary to support the achievement of objectives.
	• Evaluates Competence and Addresses Shortcomings — The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.
	• Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.
	• Plans and Prepares for Succession — Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.
	Additional point of focus specifically related to all engagements using the trust services criteria:

	• *Considers the Background of Individuals — The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Considers the Technical Competency of Individuals — The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Enforces Accountability Through Structures, Authorities, and Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.
	• Establishes Performance Measures, Incentives, and Rewards — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
	• Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance — Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.
	• Considers Excessive Pressures — Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.
	• Evaluates Performance and Rewards or Disciplines Individuals — Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and

	provide rewards or exercise disciplinary action, as appropriate.
	COMMUNICATION AND INFORMATION
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Identifies Information Requirements — A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.
	• Captures Internal and External Sources of Data — Information systems capture internal and external sources of data.
	• Processes Relevant Data Into Information — Information systems process and transform relevant data into information.
	• Maintains Quality Throughout Processing — Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.
	• Communicates With the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.

	• Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Communicates Responsibilities — Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*
	• *Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters — Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.*
	• *Communicates Objectives and Changes to Objectives — The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*
	• *Communicates Information to Improve Security Knowledge and Awareness — The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:
	• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives — The entity communicates its objectives to personnel to enable them to carry out their responsibilities.***

	• ***<u>Communicates System Changes</u> — System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.***
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• <u>Communicates to External Parties</u> — Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.
	• <u>Enables Inbound Communications</u> — Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
	• <u>Communicates With the Board of Directors</u> — Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
	• <u>Provides Separate Communication Lines</u> — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• <u>Selects Relevant Method of Communication</u> — The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.
	Additional point of focus that applies only to an engagement using the trust services criteria for confidentiality:
	• *<u>Communicates Objectives Related to Confidentiality and Changes to Objectives</u> — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*

	Additional point of focus that applies only to an engagement using the trust services criteria for privacy:
	• *Communicates Objectives Related to Privacy and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:
	• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives — The entity communicates its system objectives to appropriate external users.***
	• ***Communicates System Responsibilities — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.***
	• ***Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters — External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.***
	RISK ASSESSMENT
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	Operations Objectives

	• Reflects Management's Choices — Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
	• Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	• Includes Operations and Financial Performance Goals — The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
	• Forms a Basis for Committing of Resources — Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.
	External Financial Reporting Objectives • Complies With Applicable Accounting Standards — Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
	• Considers Materiality — Management considers materiality in financial statement presentation.
	• Reflects Entity Activities — External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.
	External Nonfinancial Reporting Objectives • Complies With Externally Established Frameworks — Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.
	• Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.
	• Reflects Entity Activities — External reporting reflects the underlying transactions and events within a range of acceptable limits.
	Internal Reporting Objectives • Reflects Management's Choices — Internal reporting provides management with accurate and complete information regarding management's choices and information

	needed in managing the entity.
	• Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
	• Reflects Entity Activities — Internal reporting reflects the underlying transactions and events within a range of acceptable limits.
	Compliance Objectives • Reflects External Laws and Regulations — Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.
	• Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Establishes Sub-objectives to Support Objectives — Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels — The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
	• Analyzes Internal and External Factors — Risk identification considers both internal and external factors and their impact on the achievement of objectives.
	• Involves Appropriate Levels of Management — The entity puts into place effective

	risk assessment mechanisms that involve appropriate levels of management.
	• Estimates Significance of Risks Identified — Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
	• Determines How to Respond to Risks — Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities — The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.*
	• *Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.*
	• *Considers the Significance of the Risk — The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.*
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers Various Types of Fraud — The assessment of fraud considers fraudulent

	reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
	• Assesses Incentives and Pressures — The assessment of fraud risks considers incentives and pressures.
	• Assesses Opportunities — The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.
	• Assesses Attitudes and Rationalizations — The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers the Risks Related to the Use of IT and Access to Information — The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.*
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Assesses Changes in the External Environment — The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
	• Assesses Changes in the Business Model — The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
	• Assesses Changes in Leadership — The entity considers changes in management and respective attitudes and philosophies on the system of internal control.

	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Assesses Changes in Systems and Technology — The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*
	• *Assesses Changes in Vendor and Business Partner Relationships — The risk identification process considers changes in vendor and business partner relationships.*
	MONITORING ACTIVITIES
CC4.1	**COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers a Mix of Ongoing and Separate Evaluations — Management includes a balance of ongoing and separate evaluations.
	• Considers Rate of Change — Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
	• Establishes Baseline Understanding — The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
	• Uses Knowledgeable Personnel — Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
	• Integrates With Business Processes — Ongoing evaluations are built into the business processes and adjust to changing conditions.
	• Adjusts Scope and Frequency — Management varies the scope and frequency of separate evaluations depending on risk.

	• Objectively Evaluates — Separate evaluations are performed periodically to provide objective feedback.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Different Types of Ongoing and Separate Evaluations — Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.*
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Assesses Results — Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
	• Communicates Deficiencies — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
	• Monitors Corrective Action — Management tracks whether deficiencies are remedied on a timely basis.
	CONTROL ACTIVITIES
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Integrates With Risk Assessment — Control activities help ensure that risk responses that address and mitigate risks are carried out.

	• Considers Entity-Specific Factors — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
	• Determines Relevant Business Processes — Management determines which relevant business processes require control activities.
	• Evaluates a Mix of Control Activity Types — Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
	• Considers at What Level Activities Are Applied — Management considers control activities at various levels in the entity.
	• Addresses Segregation of Duties — Management segregates incompatible duties and, where such segregation is not practical, management selects and develops alternative control activities.
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls — Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
	• Establishes Relevant Technology Infrastructure Control Activities — Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
	• Establishes Relevant Security Management Process Controls Activities — Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
	• Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities — Management selects and develops control activities over

	the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Establishes Policies and Procedures to Support Deployment of Management's Directives — Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
	• Establishes Responsibility and Accountability for Executing Policies and Procedures — Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
	• Performs in a Timely Manner — Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
	• Takes Corrective Action — Responsible personnel investigate and act on matters identified as a result of executing control activities.
	• Performs Using Competent Personnel — Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
	• Reassesses Policies and Procedures — Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.
	Logical and Physical Access Controls
CC6.1	***The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies and Manages the Inventory of Information Assets — The entity identifies,*

	inventories, classifies, and manages information assets.
	• *Restricts Logical Access — Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.*
	• *Identifies and Authenticates Users — Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*
	• *Considers Network Segmentation — Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*
	• *Manages Points of Access — Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*
	• *Restricts Access to Information Assets — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access-control rules for information assets.*
	• *Manages Identification and Authentication — Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.*
	• *Manages Credentials for Infrastructure and Software — New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.*
	• *Uses Encryption to Protect Data — The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.*
	• *Protects Encryption Keys — Processes are in place to protect encryption keys during generation, storage, use, and destruction.*
CC6.2	***Prior to issuing system credentials and granting system access, the entity registers and authorizes***

	new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Controls Access Credentials to Protected Assets — Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*
	• *Removes Access to Protected Assets When Appropriate — Processes are in place to remove credential access when an individual no longer requires such access.*
	• *Reviews Appropriateness of Access Credentials — The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*
CC6.3	***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Access to Protected Information Assets — Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*
	• *Removes Access to Protected Information Assets — Processes are in place to remove access to protected information assets when an individual no longer requires access.*
	• *Uses Role-Based Access Controls — Role-based access control is utilized to support segregation of incompatible functions.*
	• *Reviews Access Roles and Rules — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.*

CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Physical Access — Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*
	• *Removes Physical Access — Processes are in place to remove access to physical resources when an individual no longer requires access.*
	• *Reviews Physical Access — Processes are in place to periodically review physical access to ensure consistency with job responsibilities.*
CC6.5	***The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies Data and Software for Disposal — Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*
	• *Removes Data and Software From Entity Control — Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts Access — The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*

	• *Protects Identification and Authentication Credentials — Identification and authentication credentials are protected during transmission outside its system boundaries.*
	• *Requires Additional Authentication or Credentials — Additional authentication information or credentials are required when accessing the system from outside its boundaries.*
	• *Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*
CC6.7	***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts the Ability to Perform Transmission — Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.*
	• *Uses Encryption Technologies or Secure Communication Channels to Protect Data — Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*
	• *Protects Removal Media — Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.*
	• *Protects Mobile Devices — Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.*
CC6.8	***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Restricts Application and Software Installation — The ability to install applications and software is restricted to authorized individuals.*
	• *Detects Unauthorized Changes to Software and Configuration Parameters — Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*
	• *Uses a Defined Change Control Process — A management-defined change control process is used for the implementation of software.*
	• *Uses Antivirus and Anti-Malware Software — Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.*
	• *Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software — Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.*
	System Operations
CC7.1	***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Uses Defined Configuration Standards — Management has defined configuration standards.*
	• *Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*
	• *Implements Change-Detection Mechanisms — The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*
	• *Detects Unknown or Unauthorized Components — Procedures are in place to de-*

	tect the introduction of unknown or unauthorized components.
	• *Conducts Vulnerability Scans — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*
CC7.2	***The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Implements Detection Policies, Procedures, and Tools — Detection policies and procedures are defined and implemented and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*
	• *Designs Detection Measures — Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*
	• *Implements Filters to Analyze Anomalies — Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*
	• *Monitors Detection Tools for Effective Operation — Management has implemented processes to monitor the effectiveness of detection tools.*
CC7.3	***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Responds to Security Incidents — Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*
	• *Communicates and Reviews Detected Security Events — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*
	• *Develops and Implements Procedures to Analyze Security Incidents — Procedures are in place to analyze security incidents and determine system impact.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Assesses the Impact on Personal Information — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*
	• *Determines Personal Information Used or Disclosed — When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.*
CC7.4	***The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Assigns Roles and Responsibilities — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.*
	• *Contains Security Incidents — Procedures are in place to contain security incidents that actively threaten entity objectives.*
	• *Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.*

	• *Ends Threats Posed by Security Incidents — Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*
	• *Restores Operations — Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*
	• *Develops and Implements Communication Protocols for Security Incidents — Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*
	• *Obtains Understanding of Nature of Incident and Determines Containment Strategy — An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*
	• *Remediates Identified Vulnerabilities — Identified vulnerabilities are remediated through the development and execution of remediation activities.*
	• *Communicates Remediation Activities — Remediation activities are documented and communicated in accordance with the incident-response program.*
	• *Evaluates the Effectiveness of Incident Response — The design of incident-response activities is evaluated for effectiveness on a periodic basis.*
	• *Periodically Evaluates Incidents — Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Communicates Unauthorized Use and Disclosure — Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.*
	• *Application of Sanctions — The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance*

	with entity policies and legal and regulatory requirements.
CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restores the Affected Environment — The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*
	• *Communicates Information About the Event — Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).*
	• *Determines Root Cause of the Event — The root cause of the event is determined.*
	• *Implements Changes to Prevent and Detect Recurrences — Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*
	• *Improves Response and Recovery Procedures — Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.*
	• *Implements Incident-Recovery Plan Testing — Incident-recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	Change Management
CC8.1	***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Manages Changes Throughout the System Life Cycle — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.*
	• *Authorizes Changes — A process is in place to authorize system changes prior to development.*
	• *Designs and Develops Changes — A process is in place to design and develop system changes.*
	• *Documents Changes — A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.*
	• *Tracks System Changes — A process is in place to track system changes prior to implementation.*
	• *Configures Software — A process is in place to select and implement the configuration parameters used to control the functionality of software.*
	• *Tests System Changes — A process is in place to test system changes prior to implementation.*
	• *Approves System Changes — A process is in place to approve system changes prior to implementation.*
	• *Deploys System Changes — A process is in place to implement system changes.*
	• *Identifies and Evaluates System Changes — Objectives affected by system changes are identified and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*
	• *Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents — Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified and the change process is initiated upon identification.*
	• *Creates Baseline Configuration of IT Technology — A baseline configuration of IT*

	and control systems is created and maintained.
	• *Provides for Changes Necessary in Emergency Situations — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).*
	Additional points of focus that apply only in an engagement using the trust services criteria for confidentiality:
	• *Protects Confidential Information — The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Protects Personal Information — The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.*
	Risk Mitigation
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.*
	• *Considers the Use of Insurance to Mitigate Financial Impact Risks — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.*

CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*
	• *Assesses Vendor and Business Partner Risks — The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*
	• *Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.*
	• *Establishes Communication Protocols for Vendors and Business Partners — The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.*
	• *Establishes Exception Handling Procedures From Vendors and Business Partners — The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*
	• *Assesses Vendor and Business Partner Performance — The entity periodically assesses the performance of vendors and business partners.*
	• *Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments — The entity implements procedures for addressing issues identified with vendor and business partner relationships.*
	• *Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.*
	Additional points of focus that apply only to an engagement using the trust services criteria for confidentiality:

	• *Obtains Confidentiality Commitments from Vendors and Business Partners — The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*
	• *Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*
	Additional points of focus that apply only to an engagement using the trust services criteria for privacy:
	• *Obtains Privacy Commitments from Vendors and Business Partners — The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.*
	• *Assesses Compliance with Privacy Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.*
	ADDITIONAL CRITERIA FOR AVAILABILITY
A1.1	***The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Measures Current Usage — The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.*
	• *Forecasts Capacity — The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.*
	• *Makes Changes Based on Forecasts — The system change management process is*

	initiated when forecasted usage exceeds capacity tolerances.
A1.2	***The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services availability criteria, highlight important characteristics relating to this criterion:
	• *Identifies Environmental Threats — As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.*
	• *Designs Detection Measures — Detection measures are implemented to identify anomalies that could result from environmental threat events.*
	• *Implements and Maintains Environmental Protection Mechanisms — Management implements and maintains environmental protection mechanisms to prevent and mitigate environmental events.*
	• *Implements Alerts to Analyze Anomalies — Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.*
	• *Responds to Environmental Threat Events — Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator backup subsystem).*
	• *Communicates and Reviews Detected Environmental Threat Events — Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system and actions are taken, if necessary.*
	• *Determines Data Requiring Backup — Data is evaluated to determine whether backup is required.*
	• *Performs Data Backup — Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.*
	• *Addresses Offsite Storage — Backup data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environ-*

	mental threat event affecting both sets of data is reduced to an appropriate level.
	• *Implements Alternate Processing Infrastructure — Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.*
A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Implements Business Continuity Plan Testing — Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	• *Tests Integrity and Completeness of Backup Data — The integrity and completeness of backup information is tested on a periodic basis.*
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	***The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential information — Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.*
	• *Protects Confidential Information From Destruction — Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.*
C1.2	***The entity disposes of confidential information to meet the entity's objectives related to confidentiality.***

	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential Information for Destruction — Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.*
	• *Destroys Confidential Information — Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.*
	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY (OVER THE PROVISION OF SERVICES OR THE PRODUCTION, MANUFACTURING, OR DISTRIBUTION OF GOODS)
PI1.1	***The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Identifies Information Specifications — The entity identifies information specifications required to support the use of products and services.*
	• *Defines Data Necessary to Support a Product or Service — When data is provided as part of a service or product or as part of a reporting obligation related to a product or service:* 1. *The definition of the data is available to the users of the data* 2. *The definition of the data includes the following information:* *a. The population of events or instances included in the data* *b. The nature of each element (for example, field) of the data (that is, the event or instance to which the data element relates, for example, transaction price of a sale of XYZ Corporation stock for the last trade in that stock on a given day)* *c. Source(s) of the data* *d. The unit(s) of measurement of data elements (for example, fields)* *e. The accuracy/correctness/precision of measurement* *f. The uncertainty or confidence interval inherent in each data element and in the population of those elements* *g. The date the data was observed or the period of time during which the events relevant to the data occurred* *h. The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements*

	and population 3. *The definition is complete and accurate.* 4. *The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (metadata) that has not been included within the data.*
	The following point of focus, which applies only to an engagement using the trust services criteria for processing integrity for a system that produces, manufactures, or distributes products, highlights important characteristics relating to this criterion:
	• *Defines Information Necessary to Support the Use of a Good or Product — When information provided by the entity is needed to use the good or product in accordance with its specifications:* 1. *The required information is available to the user of the good or product.* 2. *The required information is clearly identifiable.* 3. *The required information is validated for completeness and accuracy.*
PI1.2	***The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Characteristics of Processing Inputs — The characteristics of processing inputs that are necessary to meet requirements are defined.*
	• *Evaluates Processing Inputs — Processing inputs are evaluated for compliance with defined input requirements.*
	• *Creates and Maintains Records of System Inputs — Records of system input activities are created and maintained completely and accurately in a timely manner.*
PI1.3	***The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Processing Specifications — The processing specifications that are necessary to meet product or service requirements are defined.*

	• *Defines Processing Activities — Processing activities are defined to result in products or services that meet specifications.*
	• *Detects and Corrects Production Errors — Errors in the production process are detected and corrected in a timely manner.*
	• *Records System Processing Activities — System processing activities are recorded completely and accurately in a timely manner.*
	• *Processes Inputs — Inputs are processed completely, accurately, and timely as authorized in accordance with defined processing activities.*
PI1.4	***The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Protects Output — Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting specifications.*
	• *Distributes Output Only to Intended Parties — Output is distributed or made available only to intended parties.*
	• *Distributes Output Completely and Accurately — Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output.*
	• *Creates and Maintains Records of System Output Activities — Records of system output activities are created and maintained completely and accurately in a timely manner.*
PI1.5	***The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:

	• *Protects Stored Items — Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications.*
	• *Archives and Protects System Records — System records are archived and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used.*
	• *Stores Data Completely and Accurately — Procedures are in place to provide for the complete, accurate, and timely storage of data.*
	• *Creates and Maintains Records of System Storage Activities — Records of system storage activities are created and maintained completely and accurately in a timely manner.*
	ADDITIONAL CRITERIA FOR PRIVACY
P1.0	**Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy**
P1.1	***The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects — Notice is provided to data subjects regarding the following:* — *Purpose for collecting personal information* — *Choice and consent* — *Types of personal information collected* — *Methods of collection (for example, use of cookies or other tracking techniques)* — *Use, retention, and disposal* — *Access* — *Disclosure to third parties* — *Security for privacy*

	— *Quality, including data subjects' responsibilities for quality* — *Monitoring and enforcement* *If personal information is collected from sources other than the individual, such sources are described in the privacy notice.*
	• <u>*Provides Notice to Data Subjects*</u> *— Notice is provided to data subjects (1) at or before the time personal information is collected or as soon as practical thereafter, (2) at or before the entity changes its privacy notice or as soon as practical thereafter, or (3) before personal information is used for new purposes not previously identified.*
	• <u>*Covers Entities and Activities in Notice*</u> *— An objective description of the entities and activities covered is included in the entity's privacy notice.*
	• <u>*Uses Clear and Conspicuous Language*</u> *— The entity's privacy notice is conspicuous and uses clear language.*
P2.0	**Privacy Criteria Related to Choice and Consent**
P2.1	***The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• <u>*Communicates to Data Subjects*</u> *— Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.*
	• <u>*Communicates Consequences of Denying or Withdrawing Consent*</u> *— When personal information is collected, data subjects are informed of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.*
	• <u>*Obtains Implicit or Explicit Consent*</u> *— Implicit or explicit consent is obtained from data subjects at or before the time personal information is collected or soon there-*

	after. The individual's preferences expressed in his or her consent are confirmed and implemented.
	• *Documents and Obtains Consent for New Purposes and Uses — If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.*
	• *Obtains Explicit Consent for Sensitive Information — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Obtains Consent for Data Transfers — Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.*
P3.0	**Privacy Criteria Related to Collection**
P3.1	***Personal information is collected consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Limits the Collection of Personal Information — The collection of personal information is limited to that necessary to meet the entity's objectives.*
	• *Collects Information by Fair and Lawful Means — Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.*
	• *Collects Information From Reliable Sources — Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.*
	• *Informs Data Subjects When Additional Information Is Acquired — Data subjects are informed if the entity develops or acquires additional information about them for its use.*
P3.2	***For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives re-***

	lated to privacy.
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Obtains Explicit Consent for Sensitive Information — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Documents Explicit Consent to Retain Information — Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.*
P4.0	**Privacy Criteria Related to Use, Retention, and Disposal**
P4.1	***The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Uses Personal Information for Intended Purposes — Personal information is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained, unless a law or regulation specifically requires otherwise.*
P4.2	***The entity retains personal information consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Retains Personal Information — Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.*
	• *Protects Personal Information — Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.*
P4.3	***The entity securely disposes of personal information to meet the entity's objectives related to privacy.***

	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Captures, Identifies, and Flags Requests for Deletion — Requests for deletion of personal information are captured and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.*
	• *Disposes of, Destroys, and Redacts Personal Information — Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.*
	• *Destroys Personal Information — Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.*
P5.0	**Privacy Criteria Related to Access**
P5.1	***The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Authenticates Data Subjects' Identity — The identity of data subjects who request access to their personal information is authenticated before they are given access to that information.*
	• *Permits Data Subjects Access to Their Personal Information — Data subjects are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.*
	• *Provides Understandable Personal Information Within Reasonable Time — Personal information is provided to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.*
	• *Informs Data Subjects If Access Is Denied — When data subjects are denied access to their personal information, the entity informs them of the denial and the reason for the denial in a timely manner, unless prohibited by law or regulation.*

P5.2	***The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Denial of Access Requests — Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.*
	• *Permits Data Subjects to Update or Correct Personal Information — Data subjects are able to update or correct personal information held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's personal information consistent with the entity's objectives related to privacy.*
	• *Communicates Denial of Correction Requests — Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.*
P6.0	**Privacy Criteria Related to Disclosure and Notification**
P6.1	***The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Privacy Policies to Third Parties — Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.*
	• *Discloses Personal Information Only When Appropriate — Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.*
	• *Discloses Personal Information Only to Appropriate Third Parties — Personal information is disclosed only to third parties who have agreements with the entity to*

	protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.
	• *Discloses Information to Third Parties for New Purposes and Uses — Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.*
P6.2	***The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Authorized Disclosures — The entity creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely.*
P6.3	***The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Detected or Reported Unauthorized Disclosures — The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is complete, accurate, and timely.*
P6.4	***The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Discloses Personal Information Only to Appropriate Third Parties — Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet*

	the terms of the agreement, instructions, or requirements.
	• *Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
P6.5	***The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Reports Actual or Suspected Unauthorized Disclosures — A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.*
P6.6	***The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Provides Notice of Breaches and Incidents — The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.*
P6.7	***The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.***

	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Identifies Types of Personal Information and Handling Process — The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified.*
	• *Captures, Identifies, and Communicates Requests for Information — Requests for an accounting of personal information held and disclosures of the data subjects' personal information are captured and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.*
P7.0	**Privacy Criteria Related to Quality**
P7.1	***The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Ensures Accuracy and Completeness of Personal Information — Personal information is accurate and complete for the purposes for which it is to be used.*
	• *Ensures Relevance of Personal Information — Personal information is relevant to the purposes for which it is to be used.*
P8.0	**Privacy Criteria Related to Monitoring and Enforcement**
P8.1	***The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects — Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes.*
	• *Addresses Inquiries, Complaints, and Disputes — A process is in place to address*

	inquiries, complaints, and disputes.
	• *Documents and Communicates Dispute Resolution and Recourse — Each complaint is addressed and the resolution is documented and communicated to the individual.*
	• *Documents and Reports Compliance Review Results — Compliance with objectives related to privacy are reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.*
	• *Documents and Reports Instances of Noncompliance — Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.*
	• *Performs Ongoing Monitoring — Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.*

Appendix A — Glossary

.25

access to personal information. The ability to view personal information held by an organization. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals need to be able to find out what personal information an entity has on file about them and how the information is being used. Individuals need to be able to correct erroneous information in such records.

architecture. The design of the structure of a system, including logical components, and the logical interrelationships of a computer, its operating system, a network, or other elements.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access.

board or **board of directors.** Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

business partner. An individual or business (and its employees), other than a vendor, that has some degree of involvement with the entity's business dealings or agrees to cooperate, to any degree, with the entity (for example, a computer manufacturer who works with another company who supplies it with parts).

collection. The process of obtaining personal information from the individual directly (for example, through the individual's submission of an internet form or a registration form) or from another party such as a business partner.

commitments. Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided or the product, production, manufacturing, or distribution specifications.

component. One of five elements of internal control, including the control environment, risk assessment, control activities, information and communication, and monitoring activities.

compromise. Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs.

controls. Policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

control activity. An action established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

consent. This privacy requirement is one of the fair information practice objectives. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice about the use or disclosure of his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative (for example, opting in) or implied (for example, not opting out). There are two types of consent:

- **explicit consent.** A requirement that an individual "signifies" his or her agreement with a data controller by some active communication between the parties.

- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

COSO. The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private-sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. (See www.coso.org.)

criteria. The benchmarks used to measure or evaluate the subject matter.

cybersecurity objectives. Objectives that address the cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives).

design. As used in the COSO definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of an entity's objectives.

data subject. The individual about whom personal information is collected.

disclosure. The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. Disclosure is often used interchangeably with the terms *sharing* and *onward transfer*.

disposal. A phase of the data life cycle that pertains to how an entity removes or destroys data or information.

effectiveness (of controls). Encompasses both the suitability of the design of controls and the operating effectiveness of controls to provide reasonable assurance that the entity's principal system objectives are achieved.

entity. A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, a not-for-profit organization, a government body, or an academic institution. The management operating model may follow product or service lines, divisions, or operating units, with geographic markets providing for further subdivisions or aggregations of performance.

entity-wide. Activities that apply across the entity — most commonly in relation to entity-wide controls.

environmental. Of or having to do with the matters that can damage the physical elements of information systems (for example, fire, flood, wind, earthquake, power surges, or power outages). An entity implements controls and other activities to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system from environmental elements.

external users. Users, other than entity personnel, who are authorized by entity management, customers, or other authorized persons to interact with the entity's information system.

information and systems. Refers to information in electronic form (electronic information) during its use, processing, transmission, and storage and systems that use, process, transmit or transfer, and store information or that produce, manufacture, or distribute products.

information assets. Data and the associated software and infrastructure used to process, transmit, and store information or to produce, manufacture, or distribute products.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network elements.

internal control. A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

outsourced service providers. A service provider that performs business processes, operations, or controls on behalf of the entity when such business processes, operations, or controls are necessary to achieve the entity's objectives.

personal information. Information that is or can be about or related to an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the bases for procedures.

practitioner. As used in this document, a CPA who performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

principal system objectives. System objectives that relate to the trust services category or categories addressed by the examination and that could reasonably be expected to influence the relevant decisions of intended users. (See *system objectives*.)

privacy commitments. Declarations made by management regarding the performance of a system processing personal information. Such commitments can be communicated in written agreements, standardized contracts, service level agreements, or published statements (for example, a privacy practices statement). In addition, privacy commitments may be made on many different aspects of the service being provided.

privacy notice. A written communication by entities that collect personal information, to the individuals about whom personal information is collected, about the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

products. Tangible or intangible goods manufactured or produced by an entity. Throughout this document, the term is used interchangeably with *goods.*

report users. Intended users of the practitioner's report in accordance with AT-C section 205, *Examination Engagements*. [fn 1] There may be a broad range of report users for a general-purpose report but only a limited number of specified parties for a report that is restricted in accordance with paragraph .64 of AT-C section 205.

retention. A phase of the data life cycle that pertains to how long an entity stores information for future use or reference.

[fn 1] All AT-C sections can be found in AICPA *Professional Standards*.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

risk response. The decision to accept, avoid, reduce, or share a risk.

security event. An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems.

security incident. A security event that requires action on the part of an entity in order to protect information assets and resources.

senior management. The chief executive officer or equivalent organizational leader and senior management team.

service provider. A supplier (such as a service organization) engaged to provide services to the entity. Service providers include outsourced service providers as well as suppliers that provide services not associated with business functions, such as janitorial, legal, and audit services.

SOC 2 engagement. An examination engagement to report on the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls. This engagement is performed in accordance with the attestation standards and AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

SOC 3 engagement. An examination engagement to report on the suitability of design and the operating effectiveness of an entity's controls over a system relevant to one or more of the trust services categories.

SOC for Cybersecurity examination. An examination engagement to report on whether (*a*) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria. A SOC for Cybersecurity examination is performed in accordance with the attestation standards and AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

SOC for Supply Chain examination. An examination engagement to report on whether (*a*) the description of the entity's system is presented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria. Such an examination is based on guidance contained in AICPA Guide *SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System*.

stakeholders. Parties that are affected by the entity, such as shareholders, the communities in which an entity operates, employees, customers, and suppliers.

subsequent events. Events or transactions that occur after the specified period addressed by the description but prior to the date of the practitioner's report; such events or transactions could have a significant effect on the evaluation of whether the description is presented in accordance with the description criteria or whether controls were effective to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria.

supplier. See definition for *vendor*.

system. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

system boundaries. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function (such as producing, manufacturing, or distributing a product) or provide a service. When systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap but the boundaries of each system will differ.

system components. Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and could result in an entity's failure to achieve its system objectives. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data; or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of entity management to prevent or reduce the impact of a system event on the entity's achievement of its system objectives.

system objectives. The entity's objectives, established by entity management, that are embodied in the product commitments it makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. The system objectives also include the requirements established for the functioning of the system to meet production, manufacturing, or distribution commitments.

system requirements. Specifications regarding how the system should function to (*a*) meet the entity's commitments to customers and others (such as customers' customers); (*b*) meet the entity's commitments to suppliers and business partners; (*c*) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other entity objectives that are relevant to the trust services category or categories addressed by the description. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations.

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically

enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

third party. An individual or organization other than the entity and its employees. Third parties may be customers, suppliers, business partners, or others.

trust services. A set of professional attestation and advisory services based on a core set of criteria related to security, availability, processing integrity, confidentiality, or privacy.

unauthorized access. Access to information or system components that (*a*) has not been approved by a person designated to do so by management and (*b*) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

vendor (or supplier). An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the entity that are necessary to achieve the entity's objectives), it also might be a service provider.