Chapter 1

Introduction and Background

This chapter provides examples of service organizations, describes how a service organization's controls may affect a user entity's internal control over financial reporting, and identifies other engagements performed under Statements on Standards for Attestation Engagements that involve reporting on controls.

1.01 Many entities outsource aspects of their business activities to organizations that provide services ranging from performing a specific task under the direction of the entity to replacing entire business units or functions of the entity. Many of the services provided by such organizations are integral to their customers' business operations. However, not all of those services are relevant to their customers' internal control over financial reporting and, therefore, to an audit of financial statements.

1.02 AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), uses the term *service organization* to refer to an entity to which services are outsourced. AT-C section 320 defines a service organization as "an organization or segment of an organization that provides services to user entities, which are likely to be relevant to those user entities' internal control over financial reporting." The entities that use the services of a service organization are termed *user entities*.

1.03 Services performed by service organizations and controls related to these services may affect a user entity's internal control over financial reporting. When this situation occurs, an auditor performing an audit of a user entity's financial statements (a user auditor) is required to perform risk assessment procedures to obtain an understanding of how the user entity uses the services of a service organization.

1.04 An example of the service organizations addressed by AT-C section 320 and this guide is a health insurance company that processes medical claims for other companies that have self-insured health plans. When the medical claims processing function is outsourced, the participants in the self-insured health plan are instructed to submit their claims directly to the medical claims processor. The medical claims processor processes the claims for the self-insured health plans based on rules established by the companies with the self-insured health plans, for example, rules related to eligibility and the amount to be paid for each service. The medical claims processor provides claims data to the companies that have self-insured health plans, such as the cost of claims paid during the period under examination and the cost of claims incurred during the examination period but not recorded until after the examination period. The self-insured companies use this data to record their claims expense and the related liability. That information flows through to the self-insured companies' financial statements. Controls at the claims processor will affect the quality of the data provided to the self-insured health plans. Therefore, controls at the service organization (medical claims processor) are relevant to user entities'

(companies with a self-insured health plan) internal control over financial reporting.

1.05 The following are some additional examples of service organizations that perform functions that are relevant to user entities' internal control over financial reporting:

- *Trust departments of banks.* The trust department of a bank may serve as custodian of an employee benefit plan's assets, maintain records of each participant's account, allocate investment income to the participants based on a formula in the trust agreement, and make payments to the participants. If an employee benefit plan engages a service organization to perform some or all of these tasks, the services provided by the service organization generate information that is included in the plan's financial statements.
- *Custodians for investment companies.* Custodians for investment companies are responsible for the receipt, delivery, and safekeeping of an investment company's portfolio securities; the receipt and disbursement of cash resulting from transactions in these securities; and the maintenance of records of the securities held for the investment company. The custodian may also perform other services for the investment company, such as collecting dividend and interest income and distributing that income to the investment company. The custodian is a service organization to the investment company.
- *Mortgage servicers or depository institutions that service loans for others.* Investor entities may purchase mortgage loans or participation interests in such loans from thrifts, banks, or mortgage companies. These loans become assets of the investor entities, and the sellers may continue to service the loans. Mortgage servicing activities generally include collecting mortgage payments from borrowers, conducting collection and foreclosure activities, maintaining escrow accounts for the payment of property taxes and insurance, paying taxing authorities and insurance companies as payments become due, remitting monies to investors (user entities), and reporting data concerning the mortgage to user entities. The user entities may have little or no contact with the mortgage servicer other than receiving the monthly payments and reports from the mortgage servicer. The user entities record transactions related to the underlying mortgage loans based on data provided by the mortgage servicer.
- *Application service providers (ASPs).* ASPs provide packaged software applications and a technology environment that enables customers to process financial and operational transactions. An ASP may specialize in providing a particular software package solution to its users, may perform business processes for user entities that the user entities had traditionally performed themselves, or may provide some combination of these services. As such, an ASP may be a service organization if it provides services that are part of the user entity's information system.
- *Regional transmission organizations (RTOs).* These are entities in the electric utility industry (also referred to as independent system operators) that are responsible for the operation of a centrally

dispatched electric system or wholesale electric market. They are also responsible for initiating, recording, billing, settling, and reporting transactions, as well as collecting and remitting cash from participants based on the transmission tariff or other governing rules. These services may be part of a participant's information system, therefore making the RTO a service organization.

1.06 Some service organizations provide services and implement controls that are relevant to subject matter other than user entities' internal control over financial reporting. Paragraph .04 of AT-C section 320 indicates that, although AT-C section 320 focuses on controls at service organizations likely to be relevant to user entities' internal control over financial reporting, the guidance in AT-C section 320 may also be helpful to a practitioner performing an engagement under AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), to report on controls at a service organization other than those that are likely to be relevant to user entities' internal control over financial reporting. An example of such an engagement is an examination of controls over the security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by the system performed under AT-C section 205 and the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*. Paragraph 1.09 of this guide contains a table that provides examples of engagements to report on controls other than those relevant to user entities' internal control over financial reporting and the professional standard or interpretive guidance that addresses or provides a framework for each engagement.

1.07 AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization* (AICPA, *Professional Standards*), addresses the user auditor's responsibility for obtaining sufficient appropriate audit evidence in an audit of the financial statements of a user entity that uses one or more service organizations. User auditors should be aware that paragraph .05 of AU-C section 402 indicates that AU-C section 402 does not apply to the following:

- Services that are limited to processing an entity's transactions that are specifically authorized by the entity, such as the processing of checking account transactions by a bank or the processing of securities transactions by a broker (that is, when the user entity retains responsibility for authorizing the transactions and maintaining the related accountability)
- The audit of transactions arising from an entity that holds a proprietary financial interest in another entity, such as a partnership, corporation, or joint venture, when the partnership, corporation, or joint venture performs no processing on behalf of the entity

1.08 In addition to controls that affect user entity's internal control over financial reporting, a service organization implements controls that are relevant to its own internal control over financial reporting, not to the services it provides to user entities. This guide focuses only on those controls at service organizations that are likely to be relevant to user entities' internal control over financial reporting, whether or not they may be relevant to the service organization's own financial reporting objectives.

Other Types of Internal Control Engagements

1.09 Many attestation engagements that involve reporting on controls or internal control are not performed under AT-C section 320. Table 1-1 is intended to assist practitioners in determining the applicable attestation standard or interpretive guidance to be used when reporting on controls in a variety of circumstances.

Table 1-1

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
Reporting on controls at a service organization relevant to user entities' internal control over financial reporting: • Controls were not designed by the service organization, and • Management of the service organization — will not provide an assertion regarding the suitability of the design of the controls — will provide an assertion regarding the fairness of the presentation of the description and the operating effectiveness of the controls	Report on the fairness of the presentation of the description under AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), using the description criteria in paragraph .15 of AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), and adapting the relevant requirements and guidance therein.	Use of this report is restricted to management of the service organization, user entities, and the auditors of the user entities' financial statements.

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls—*continued*

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
This examination report includes management's description of the service organization's system[1] and a description of the service auditor's tests of controls and results.	Report on an examination of the operating effectiveness of the controls under AT-C section 205 or	AT-C section 205 Use of this report is restricted to management of the service organization, user entities, and the auditors of the user entities' financial statements.
The agreed-upon procedures report includes a description of the agreed-upon procedures performed by the practitioner and the practitioner's findings.	Report on the agreed-upon procedures performed under AT-C section 215, *Agreed-Upon Procedures Engagements* (AICPA, *Professional Standards*).	AT-C section 215 Use of this report is restricted to the specified parties that agreed upon the sufficiency of the procedures for their purposes.
Reporting on controls at a service organization relevant to user entities' internal control over financial reporting: • Controls were not designed by the service organization and	Report on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a type 2 report,[2] the operating effectiveness of the controls under AT-C section 320	Use of this report is restricted to management of the service organization, user entities, and the auditors of the user entities' financial statements.

(continued)

[1] AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting* (AICPA, *Professional Standards*), defines the term *service organization's system* as

> The policies and procedures designed, implemented, and documented by management of the service organization to provide user entities with the services covered by the service auditor's report. Management's description of the service organization's system identifies the services covered, the period to which the description relates (or in the case of a type 1 report, the date to which the description relates), the control objectives specified by management or an outside party, the party specifying the control objectives (if not specified by management), and the related controls.

[2] See paragraph 2.12 of this guide for a definition of the term *Management's description of a service organization's system and a service auditor's report on that description and on the suitability of the design and operating effectiveness of controls*, which is referred to as a *type 2 report*.

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls—*continued*

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
• Management of the service organization will provide an assertion regarding the suitability of the design of the controls (in addition to its assertion regarding the fairness of the presentation of the description of the service organization's system and the operating effectiveness of the controls).		
Reporting on controls at a service organization relevant to security availability, processing integrity, confidentiality, or privacy This report includes management's description of the service organization's system, and in a type 2 report, includes a description of service auditor's tests of controls and results (SOC 2® engagement)	Report on the fairness of the presentation of the description of the service organization's system; the suitability of the design of the controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy; and in a type 2 report, the operating effectiveness of those controls under AT-C section 205 and the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*	Use of this report is restricted to parties that are knowledgeable about • the nature of the service provided by the service organization. • how the service organization's system interacts with user entities, subservice organizations, and other parties. • internal control and its limitations. • the criteria and how controls address those criteria. • complementary user entity controls and how they interact with related controls at the service organization.

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls—*continued*

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
Reporting on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. The examination report does not include a description of the service organization's system or a description of the practitioner's tests of controls and results (SOC 3® engagement)	Report on whether the entity has maintained effective controls over its system with respect to security, availability, processing integrity, confidentiality, or privacy under AT-C section 205 and TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*)	This is a general-use report.[3]
Reporting on a service provider's controls to achieve compliance control objectives relevant to SEC Rule 38a-1, "Compliance Procedures and Practices of Certain Investment Companies,"[4] and SEC Rule 206(4)-7, "Compliance Procedures and Practices"[5]		

(continued)

[3] The term *general use* refers to reports for which use is not restricted to specified parties.

[4] Code of Federal Regulations (CFR), Title 17, Section 270.38a-1.

[5] 17 CFR 275.206(4)-7.

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls—*continued*

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
Reporting on the suitability of the design and operating effectiveness of a service provider's controls over compliance that may affect user entities' compliance This examination report does not include a description of the service organization's system or a description of the practitioner's tests of controls and results.	Report under AT-C section 205 and Statement of Position (SOP) 07-2, *Attestation Engagements That Address Specified Compliance Control Objectives and Related Controls at Entities that Provide Services to Investment Companies, Investment Advisers, or Other Service Providers* (AICPA, *Professional Standards*, AUD section 40)	Use of this report is restricted to chief compliance officers, management, boards of directors, and independent auditors of the service provider and of the entities that use the services of the service provider.
Performing agreed-upon procedures as referred to in paragraph .05 of AT-C section 320		
Performing and reporting on the results of agreed-upon procedures related to the controls of a service organization or to transactions or balances of a user entity maintained by a service organization This agreed-upon procedures report does not include a description of the service organization's system. It does include a description of the agreed-upon procedures performed by the practitioner and the practitioner's findings.	Report under AT-C section 215	Use of this report is restricted to the specified parties that agreed upon the sufficiency of the procedures for their purposes.

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls—*continued*

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
Reporting on controls over compliance with laws and regulations		
Reporting on the effectiveness of an entity's internal control over compliance with the requirements of specified laws, regulations, rules, contracts, or grants. This examination report does not include a description of the service organization's system or a description of the practitioner's tests of controls and results.	Report under AT-C section 205	Use of this report is restricted in the following circumstances: *a.* The practitioner determines that the criteria used to evaluate the subject matter are appropriate only for a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria. *b.* The criteria used to evaluate the subject matter are available only to specified parties. *c.* The engaging party is not the responsible party, and the responsible party does not provide the written representations required by paragraph .50 of AT-C section 205, but does provide oral responses to the practitioner's inquiries about the matters in paragraph .50 of AT-C section 205, as provided for in paragraphs .51 and .56*a* of AT-C section 205. In this case, the use of the practitioner's report should be restricted to the engaging party.

(continued)

Determining the Applicable Attestation Standard or Interpretive Guidance When Reporting on Controls—*continued*

Nature of the Engagement	*Professional Standard or Other Guidance*	*Restrictions on the Use of the Report*
Performing and reporting on the results of applying agreed-upon procedures related to an entity's internal control over compliance with specified requirements	Report under the applicable paragraphs of AT-C section 315, *Compliance Attestation* (AICPA, *Professional Standards*)	Use of this report is restricted to the specified parties that agreed upon the sufficiency of the procedures for their purposes.
Reporting on an entity's internal control over financial reporting in an integrated audit		
Reporting on the design and operating effectiveness of an entity's internal control over financial reporting that is integrated with an audit of financial statements	Report under AU-C section 940, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements* (AICPA, *Professional Standards*)	This is a general-use report.
This audit report does not include a description of the entity's system of internal control or a description of the auditor's tests of controls and results.		

