Information for Management of a Service Organization

AICPA Service Organization Control Reports

AICPA

SERVICE ORGANIZATIONS

SOC

aicpa.org/soc

Formerly SAS 70 Reports ®

Introduction and Background

Many entities function more efficiently and profitably by outsourcing tasks or entire functions to other organizations that have the personnel, expertise, equipment, or technology to accomplish these tasks or functions. This guide focuses on organizations that collect, process, transmit, store, organize, maintain, or dispose of information for other entities. In this guide, an organization, or segment of an organization, provides services to other entities (including operating an information system for another entity) is known as a *service organization*, and entities that use the services of service organizations are known as *user entities*. Examples of the services provided by such 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.

- *Sales force automation*. Providing and maintaining software to automate business tasks for user entities that have a sales force. Examples of such tasks are order processing, information sharing, order tracking, contact management, customer management, sales forecast analysis, and employee performance evaluation.

- *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).

One of the critical roles of management and those charged with governance in any entity is to identify and assess risks to the entity and address such risks through effective internal control. When an entity outsources tasks or functions to a service organization and becomes a user entity, it shifts some of the risks associated with performing those tasks or functions with risks associated with outsourcing, particularly risks related to how the service organization performs the tasks or functions and how that may affect the user entity's compliance with requirements. However, even though a task or function is outsourced, management of the user entity retains the ultimate responsibility for managing these risks and needs to monitor the services provided by the service organization.

To carry out its responsibilities related to the outsourced tasks or functions, management of a user entity needs information about the system by which the service organization provides services, including the service organization's controls [fn 1] over that system. User-entity management may also need assurance that the system information provided by the service organization is accurate and that the service organization actually operates in accordance with that information.

To obtain assurance, user entities often ask the service organization for a CPA's report on the service organization's system. Historically, such requests have focused on controls at the service organization that affect user entities' financial reporting. However, user entities are now requesting reports that address the security, availability, or processing integrity of the system or the confidentiality or privacy of the information processed by the system. In this document, these attributes of a system are referred to as *principles*.

CPAs (service auditors) may perform to the various types of engagements when reporting on controls at a service organization, usually referred to as *Service Organization Controls Reports*®. The following three types of Service Organization Controls Reports® are designed to help CPAs meet specific service organization and users' needs regarding internal controls at a service organization:

- *SOC 1® report*. These reports are intended to meet the needs of entities that use service organizations (user entities) and the service auditors who audit the user entities' financial statements (user auditors) when evaluating the effect of controls at the service organization on the user entities' financial statements. User auditors use these reports to plan and perform audits of the user entities' financial statements. SOC 1® engagements are performed in accordance with AT section 801, *Reporting on Controls at a Service Organization* (AICPA, *Professional Standards*), and the AICPA Guide *Reporting on Controls at a Service Organization Relevant to User Entities' Internal Controls Over Financial Reporting.*

- *SOC 2® report*. These reports are intended to meet the needs of a broad range of users who need information and assurance about controls at a service organization that affect the security, availability, or processing integrity of the systems that the service organization uses to process users' data or the confidentiality or privacy of the information processed by these systems. Examples of stakeholders who may need these reports are management or those charged with governance of the user entities and service organization, customers or suppliers of the service organization, regulators, business partners, and others who have an understanding of the service organization and its controls. These reports include a detailed description of the service organization's system; the criteria in TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*),

[fn 1] From a governance and internal control perspective, *controls* are policies and procedures that address risks associated with financial reporting, operations, or compliance and, when operating effectively, enable an entity to meet specified criteria.

applicable to the principle being reported on; the controls designed to meet these criteria; a written assertion by management regarding the description and the design and operation of the controls; and a service auditor's report in which the service auditor expresses an opinion on whether the description is fairly presented and the controls are suitability designed and operating effectively. The report also includes the service auditor's description of tests performed and results of the tests. These reports can play an important role in the following:

— Vendor management programs [fn 2]

— Internal corporate governance and risk management processes

— Regulatory compliance

These engagements are performed in accordance with AT section 101, *Attest Engagements* (AICPA, *Professional Standards*). The AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (SOC 2® guide) contains performance and reporting guidance for these engagements.

- *SOC 3® report*. These reports are designed to meet the needs of a wider range of users who need assurance about controls at a service organization that affect the security, availability, or processing integrity of the systems used by a service organization to process users' information, or the confidentiality or privacy of that information, but do not have the need for or knowledge necessary to effectively use a SOC 2® report. These reports comprise a written assertion by management regarding the suitability of the design and operating effectiveness of the controls, a service auditor's report on the suitability of the design and operating effectiveness of the controls, and a description of the system and its boundaries. This description generally is brief and does not include the detail provided in a SOC 2® system description. The criteria for evaluating the controls are the criteria in TSP section 100 that are relevant to the principle being reported on (the same criteria as in a SOC 2® report). Because they are general-use reports, SOC 3® reports can be freely distributed or posted on a website. SOC 3® engagements are performed in accordance with AT section 101.

The Trust Services Principles

The following are the trust services principles:

a. *Security*. The system is protected against unauthorized access, use, or modification.

[fn 2] *Vendor management*, in this context, is a user entity's management of the services provided by a service organization.

b. *Availability*. The system is available for operation and use as committed or agreed.

c. *Processing integrity*. System processing is complete, valid, accurate, timely, and authorized.

d. *Confidentiality*. Information designated as confidential is protected as committed or agreed.

e. *Privacy*. Personal information [fn 3] is collected, used, retained, disclosed, and disposed of in accordance with the commitments in the entity's privacy notice and criteria set forth in *Generally Accepted Privacy Principles* (GAPP) issued jointly by the AICPA and CPA Canada. (The criteria in GAPP are the same as the criteria for the privacy principle in TSP section 100.)

In a SOC 2® engagement, management of the service organization selects the trust services principle(s) that will be covered by the SOC 2® report. The trust services criteria for the principle(s) covered by the report are referred to as the *applicable trust services criteria*.

Service organization management implements controls over its systems to prevent adverse events from occurring or to detect such events as errors, privacy breaches, and theft or loss of information. For example, a control that disables a user entity's access to a system after three unsuccessful log-in attempts is designed to reduce the risk of unauthorized access to the system. Management of the service organization may engage a service auditor to report on the design and operating effectiveness of the controls over its systems. Controls that are suitably designed are able to meet the criteria they were designed to meet if they also are operating effectively. Therefore, controls that are operating effectively actually do meet the criteria they were designed to meet over a period of time.

The SOC 2® guide provides guidance to a service auditor examining and reporting on the fairness of the presentation of a description of a service organization's system; the suitability of the design of the service organization's controls over the system as they relate to one or more of the trust services principles; and, in certain reports, the operating effectiveness of those controls. This appendix is intended to

- assist management of a service organization in preparing its description of the service organization's system, which serves as the basis for a SOC 2® examination engagement.

- familiarize management with its responsibilities when it engages a service auditor to perform a SOC 2® engagement.

This appendix is not intended to provide guidance to

[fn 3] *Personal information* (sometimes referred to as *personally identifiable information*) is information that is about, or can be related to, an identifiable individual.

- management of a service organization in preparing the description of a service organization's system for a SOC 1® or SOC 3® report.

- management of a user entity in assessing a service organization's controls that are likely to be relevant to user entities' internal control over financial reporting.

- auditors of user entities (user auditors) in planning and performing an audit of a user entity's financial statements.

In the remainder of this appendix, references to *controls over a system* mean controls over a system related to one or more of the trust services principles.

Responsibilities of Management of a Service Organization

In a SOC 2® engagement, management of a service organization is responsible for the following:

- Preparing its description of the service organization's system and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion

- Providing a written assertion that accompanies management's description of the service organization's system, both of which will be provided to users of the report

- Having a reasonable basis for its assertion

- Designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the applicable trust services criteria are met

- Selecting the criteria to be used and stating them in the assertion

- Specifying any additional criteria, stating them in the description of the service organization's system, and, if the criteria are specified by law, regulation, or another party (for example, a user group or a professional body), identifying in the description the party specifying the criteria

- Identifying the risks that threaten the achievement of the criteria

- Providing the service auditor with the following:

  — Access to all information, such as records and documentation, including service-level agreements, of which management is aware, that is relevant to the description of the service organization's system and the assertion

  — Access to additional information that the service auditor may request from management for the purpose of the SOC 2® engagement

  — Unrestricted access to persons within the appropriate parties (for example, service organization personnel and subservice organization personnel) from whom the service auditor determines it is necessary to obtain evidence relevant to the service auditor’s engagement

Management of the service organization usually acknowledges these responsibilities in an engagement letter or similar written communication.

Determining the Type of Engagement to Be Performed

This guide provides for the following two types of SOC 2® engagements and related reports:

- Report on management’s description of a service organization’s system and the suitability of the design of controls (referred to as a *type 1 report*)

- Report on management’s description of a service organization’s system and the suitability of the design and operating effectiveness of controls (referred to as a *type 2 report*)

Both type 1 and type 2 reports include the following:

- Management’s description of the service organization’s system

- A written assertion by management of the service organization about the matters in the first paragraph of the section of this appendix titled “Providing a Written Assertion”

- A service auditor’s report that expresses an opinion on the matters in the first paragraph of the section of this appendix titled “Providing a Written Assertion”

A type 2 report also contains a description of the service auditor’s tests of the controls and the results of the tests.

Management’s written assertion is attached to the description of the service organization’s system.

A type 1 report, which does not include tests of the operating effectiveness of controls, provides user entities with information that will enable them to understand and assess the design of the controls. However, a type 1 report does not provide sufficient information for user entities to assess the operating effectiveness of the controls. A type 1 report may be useful if the service organization [fn 4]

[fn 4] A user of a type 1 report may misunderstand the nature of the engagement and incorrectly assume that controls are operating effectively, even though the service auditor has not provided such an opinion or performed sufficient procedures to express such an opinion. When the report user is a regulatory agency or body, this misunderstanding may result in regulatory compliance risk, particularly in a report that addresses the privacy principle.

- has not been in operation for a sufficient length of time to enable the service auditor to gather sufficient appropriate evidence regarding the operating effectiveness of controls.

- has recently made significant changes to the system and related controls and does not have a sufficient history with a stable system to enable a type 2 engagement to be performed.

Defining the Scope of the Engagement

In determining the scope of a SOC 2® engagement, management of a service organization considers the following:

- The services, business units, functional areas, business processes, and activities or applications that will be of interest to users because of concerns regarding compliance with laws, regulations, or governance or because the service organization has made commitments or agreements to user entities to provide a type 1 or type 2 report.

- The trust services principles that will be covered by the report. Management makes this determination by understanding the needs of report users and the service organization's goals in engaging a service auditor to perform the examination. The engagement may cover one, multiple, or all the principles.

- Frequency with which the report is to be issued.

- The period to be covered by the description and report (for a type 1 report, this would be the "as of" date of the description and report).

- Whether controls at subservice organizations are relevant to meeting one or more of the applicable trust services criteria. (Subservice organizations may be separate entities from the service organization or entities related to the service organization.)

To increase the likelihood that the description and service auditor's report will be useful to report users, management of the service organization may decide to discuss with user entities matters such as the services, trust services principles, and period or as of date to be covered by the description and service auditor's report.

If a service organization uses a subservice organization, the description of the service organization's system may either (*a*) include the subservice organization's services by using the inclusive method or (*b*) exclude the subservice organization's services by using the carve-out method.

When the carve-out method is used, management's description of the service organization's system identifies the nature of the services and functions performed by the subservice organization and the types of controls that management expects to be implemented at the subservice organization but excludes details of the subservice organization's system and controls.

A service organization's description prepared using the carve-out method generally is most useful if the services provided by the subservice organization are not extensive or if a type 1 or type 2 report that meets the needs of user entities is available from the subservice organization.

When the inclusive method is used, management's description of the service organization's system includes a description of the nature of the services and functions performed by the subservice organization, as well the applicable trust services criteria and controls implemented by the subservice organization. Controls of the service organization are presented separately from those of the subservice organization.

Although the inclusive method provides more information for user entities, it may not be appropriate or feasible in all circumstances. In determining which approach to use, the service organization considers (*a*) the nature and extent of the information about the subservice organization that user entities may need and (*b*) the practical difficulties entailed in implementing the inclusive method.

The inclusive method is difficult to implement in certain circumstances. The approach entails extensive planning and communication among the service auditor, the service organization, and the subservice organization. If a service organization uses the inclusive method of presentation, matters such as the following generally will need to be coordinated by all the parties involved, preferably in advance:

- The scope of the description and the timing of the examination and tests of controls
- Responsibility for preparing the section of the description that relates to the services provided by the subservice organization
- The content of the subservice organization's written representations and the members of the subservice organization's management who will be responsible for the written representations
- An agreement regarding access to the subservice organization's premises, personnel, and systems
- Fees
- Identification of the parties for whom use of the report is intended

These issues become more complex if multiple subservice organizations are involved, and the inclusive method is used. The inclusive approach is facilitated if the service organization and subservice organization are related parties or have a contractual relationship that provides for inclusive reports and visits by service auditors.

If more than one subservice organization is relevant to user entities, management of the service organization may use the inclusive method for one or more subservice organizations and the carve-out method for one or more of the other subservice organizations.

If the service organization uses the inclusive method, the service organization would obtain a written assertion from management of the subservice organization covering the subservice organization's services. That assertion would also be attached to the description of the service organization's system. If management of the subservice organization will not provide a written assertion, the service organization cannot use the inclusive method but may, instead, be able to use the carve-out method.

If the service organization's controls and monitoring of the activities of a subservice organization are sufficient to meet the applicable trust services criteria, the controls at the subservice organization are not necessary to meet those criteria. In such instances, the service organization's assertion is based solely on controls at the service organization, and consequently, neither the inclusive nor carve-out method is applicable. In these situations, the description need not describe the subservice organization's activities, unless such information is needed to help users understand the service organization's system.

Preparing the Description of the Service Organization's System

Management of a service organization is responsible for preparing the description, including the completeness, accuracy, and method of presentation of the description. No one particular format for the description is prescribed, and the extent of the description may vary depending on the size and complexity of the service organization and its activities. The description may be presented using various formats, such as narratives, flowcharts, tables, and graphics, but should meet the criteria set forth in the section of this appendix titled "Criteria for Management's Description of the Service Organization's System."

Appendix B, "Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy," of this guide contains the criteria for each of the trust services principles. All the criteria related to the trust services principle(s) being reported on (applicable trust services criteria) should be included in management's description. For example, if a service auditor is reporting on the design and operating effectiveness of controls at a service organization relevant to the availability of user entities' systems, all the controls related to the common criteria, plus the controls related to the additional criteria for availability, should be addressed by the description. If the description does not describe controls for one or more criteria, the description should include an explanation of why such criteria are not addressed by a control. Omission of controls related to one or more of the applicable trust services criteria would be appropriate if the omitted criteria are not applicable to the services provided by the service organization.

For example, in an engagement to report on the privacy principle in which personal information is collected from individuals by user entities, not the service organization, it would be appropriate to omit controls for the criteria related to collection and describe the reason for such omission. However, a policy prohibiting certain activities is not sufficient to render a criterion not applicable. For example, in a SOC 2® report that addresses the privacy principle, it would not be appropriate for a service organization to state that the criteria related to disclosure of personal information to third parties is not applicable based only on the fact that the service organization's policies forbid such disclosure. Such policies and related controls would need to be suitably designed, implemented, and operating effectively to conclude that they prevent or detect such disclosure.

The description need not address every aspect of the service organization's system or the services provided to user entities. Certain aspects of the services provided may not be relevant to user entities or may be beyond the scope of the engagement. For example, a service organization's processes related to availability are not likely to be relevant in an engagement that addresses only the security principle. Similarly, although the description should include procedures within both manual and automated systems by which services are provided, it need not necessarily include every step in the process.

The description needs to meet certain criteria in order to be fairly presented. These criteria are set forth in the section of this appendix titled "Criteria for Management's Description of the Service Organization's System." As a part of the SOC 2® engagement, the service auditor evaluates the fairness of the presentation of the description using these criteria.

Providing a Written Assertion

Management of the service organization prepares a written assertion to be attached to the description of the service organization's system. In its assertion, management confirms, to the best of its knowledge and belief, that

a. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period, based on the criteria in the section of this appendix titled "Criteria for Management's Description of the Service Organization's System."

b. the controls stated in management's description of the service organization's system were suitably designed throughout the specified period to meet the applicable trust services criteria.

c. the controls stated in management's description of the service organization's system operated effectively throughout the specified period to meet the applicable trust services criteria (type 2 report only).

Paragraph .23 of AT section 101 requires that criteria be available to users. Because the criteria in paragraphs 1.26–.27 of this guide may not be readily available to report users, management of the service organization should include in its assertion all the description criteria in paragraphs 1.26–.27 of this guide. Although all the criteria should be included in management's assertion, certain description criteria may not be pertinent to a particular service organization or system, for example, the criterion in paragraph 1.26*a*(v) would not be pertinent to a service organization that does not prepare and deliver reports or other information to user entities or other parties, and the criterion in paragraph 1.26*a*(vi)(2) would not be pertinent to a service organization that does not use a subservice organization. If certain description criteria are not pertinent to a service organization, report users generally find it useful if management presents all the description criteria and indicates which criteria are not pertinent to the service organization and the reasons therefore. Management may do so either in its system description or in a note to the specific description criteria.

Management of the service organization needs to have a reasonable basis for its written assertion, which typically is based on management's monitoring activities and other procedures.

Management's monitoring activities may provide a portion of the basis for making its assertion regarding the design and operating effectiveness of controls or may be a sufficient basis on its own. Monitoring of controls is a process to assess the effectiveness of internal control performance over time. It involves assessing the effectiveness of controls on a timely basis, identifying and reporting deficiencies to appropriate individuals within the service organization, and taking necessary corrective actions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory activities. Internal auditors or personnel performing similar functions may contribute to the monitoring of a service organization's activities. Monitoring activities may also include using information communicated by external parties, such as customer complaints and regulator comments, which may indicate problems or highlight areas in need of improvement. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. Usually, some combination of ongoing monitoring and separate evaluations will help ensure that internal control maintains its effectiveness over time. The service auditor's report on controls is not a substitute for the service organization's own processes that provide a reasonable basis for its assertion.

When monitoring does not provide a basis for management's assertion regarding the design and operating effectiveness of controls, service organization management may need to perform its own tests of the service organization's controls.

Additional Management Responsibilities

The following are some of the additional responsibilities that management of the service organization will have throughout the engagement:

- Providing access to all information, such as information in records, documentation, service-level agreements, internal audit reports, and other reports that management is aware of, that is relevant to the description of the service organization's system or the design and operating effectiveness of controls and management's assertion.

- Providing additional information that the service auditor may request from management for the purpose of the examination engagement.

- Providing unrestricted access to personnel within the service organization from whom the service auditor determines it is necessary to obtain evidence relevant to the service auditor's engagement.

- Disclosing to the service auditor any deficiencies in the design of controls of which management is aware.

- Disclosing to the service auditor all instances of which management is aware when controls have not operated with sufficient effectiveness to meet the applicable trust services criteria.

- Disclosing to the service auditor incidents of noncompliance with laws and regulations, fraud, or uncorrected errors attributable to management or other service organization personnel that are clearly not trivial and may affect one or more user entities and whether such incidents have been communicated appropriately to affected user entities.

- Selecting the criteria to be used and stating them in the assertion.

- Specifying the controls, stating them in the description of the service organization's system, and, if the controls are specified by law, regulation, or another party, identifying in the description the party specifying the controls.

- Identifying the risks that threaten the achievement of the applicable trust services criteria stated in the description and designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that the applicable trust services in the description of the service organization's system will be achieved.

- Providing written representations at the conclusion of the engagement. When the inclusive method is used, management of the service organization and subservice organization are responsible for providing separate representations. In its representations, management includes statements that

  — reaffirm its written assertion attached to the description.

  — the service organization has provided the service auditor with all relevant information and the access agreed to.

  — the service organization has disclosed to the service auditor any of the following of which it is aware:

    - Instances of noncompliance with laws or regulations or uncorrected errors attributable to the service organization that may affect one or more user entities

    - Knowledge of any actual, suspected, or alleged intentional acts by management of the service organization or its employees that could adversely affect the fairness of the presentation of management's description of the service organization's system or whether the controls stated in the description were suitably designed and operating effectively to meet the applicable trust services criteria

    - Deficiencies in the design of controls

- Instances when controls have not operated as described
- Any events subsequent to the period covered by management's description of the service organization's system up to the date of the service auditor's report that could have a significant effect on management's assertion or the fact that no such subsequent events have occurred

Criteria for Management's Description of the Service Organization's System

The criteria for determining whether the description of the service organization's system is fairly presented are as follows:

a. The description contains the following information:

i. The types of services provided.

ii. The components of the system used to provide the services, which are as follows:

(1) *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).

(2) *Software*. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).

(3) *People*. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

(4) *Procedures*. The automated and manual procedures.[fn5]

(5) *Data*. Transaction streams, files, databases, tables, and output used or processed by the system.

iii. The boundaries or aspects of the system covered by the description

iv. For information provided to, or received from, subservice organizations and other parties

(1) how the information is provided or received and the role of the subservice organizations and other parties

[fn5] The description of the procedures of the system includes those by which services are provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, delivered, and reports and other information prepared.

(2) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

v. The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:

(1) Complementary user entity controls contemplated in the design of the service organization's system

(2) When the inclusive method is used to present a subservice organization, controls at the subservice organization

vi. If the service organization presents the subservice organization using the carve-out method

(1) the nature of the services provided by the subservice organization

(2) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria

vii. Any applicable trust services criteria that are not addressed by a control and the reasons

viii. In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description

b. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to its own particular needs.

For the engagement to report on the privacy principle:

a. The types of personal information collected from individuals or obtained from user entities or other parties[6] and how such information is collected and, if collected by user entities, how it is obtained by the service organization

[6] An example of an entity that collects personal information from user entities is a credit reporting bureau that maintains information about the creditworthiness of individuals.

b. The process for

   i. identifying specific requirements in agreements with user entities and in laws and regulations applicable to the personal information and

   ii. implementing controls and practices to meet those requirements

c. If the service organization presents the subservice organization using the carve-out method

   i. any aspect of the personal information life cycle for which responsibility has been delegated to the subservice organization

   ii. the types of activities the subservice organization would need to perform to comply with the service organization's privacy commitments

d. If the service organization provides a privacy notice to individuals about whom personal information is collected, used, retained, disclosed, and disposed of or anonymized in delivering its services, the privacy notice prepared in accordance with the relevant criteria for a privacy notice set forth in TSP section 100 or a description of how the privacy notice may be obtained

e. If the service organization does not provide and is not required by law, regulation, or commitments to provide the privacy notice to individuals, a statement that the service organization is not responsible for providing a privacy notice and describes how it communicates its privacy-related commitments and practices to user entities, which includes the following information:

   i. A summary of the significant privacy-related commitments common to most agreements between the service organization and its user entities and any requirements in a particular user entity's agreement that the service organization meets for all or most user entities

   ii. A summary of the significant privacy-related requirements mandated by law, regulation, an industry, or a market that are not included in user entity agreements but the service organization meets for all or most user entities

   iii. The purposes, uses, and disclosures of personal information as permitted by user entity agreements and beyond those permitted by such agreements but not prohibited by such agreements and the service organization's commitments regarding the purpose, use, and disclosure of personal information that are prohibited by such agreements

   iv. A description of the service organization's practices regarding the retention of personal information

   v. A description of the service organization's practices for disposing of personal information

vi. If applicable, how the service organization supports any process permitted by user entities for individuals to obtain access to their information to review, update, or correct it

vii. If applicable, a description of the process to determine that personal information is accurate and complete and how the service organization implements correction processes permitted by user entities

viii. If applicable, how inquiries, complaints, and disputes from individuals (whether directly from the individual or indirectly through user entities) regarding their personal information are handled by the service organization

ix. A statement regarding the existence of a written security program and what industry or other standards it is based on

x. Other relevant information related to privacy practices deemed appropriate for user entities by the service organization