
Appendix A

Illustrative Type 2 Reports

Although 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*), specifies the components of a type 1 and type 2 report¹ and the information to be included in each component, it does not specify how the components should be organized within the type 1 or type 2 report. Service organizations and service auditors may organize and present the required information in a variety of formats. The format presented in this appendix is meant to be illustrative rather than prescriptive.

This appendix contains two illustrative type 2 reports that contain all of the required components of a type 2 report; however, for brevity, the illustrative reports do not include all the elements that might be described in a type 2 report. Ellipses (...) or parenthetical notes to readers indicate places where detail has been omitted from the illustrative reports.

The control objectives and controls specified by the service organization in examples 1 and 2, as well as the tests performed by the service auditor, are presented for illustrative purposes only. They are not intended to represent a complete or standard set of control objectives, controls, or tests of controls that would be appropriate for all service organizations. The determination of the appropriate control objectives, controls, and tests of controls for a specific service organization can be made only in the context of specific facts and circumstances. Accordingly, it is expected that actual type 2 reports will contain differing control objectives, controls, and tests of controls that are tailored to the service organization that is the subject of the engagement.

In examples 1 and 2 of this appendix, the components of the illustrative type 2 reports are referred to as "sections"; for example, section 2 contains management's assertion.

The following table identifies features of each illustrative type 2 report included in this appendix.

¹ The required components of a type 1 report are the service auditor's report, management of the service organization's written assertion, and management's description of the service organization's system. The required components of a type 2 report are the service auditor's report, management of the service organization's written assertion, management's description of the service organization's system, and the service auditor's description of tests of controls and results thereof.

Summary of Features of Illustrative Type 2 Reports in Appendix A

Number of Example and Name of Service Organization	Type of System Provided by the Service Organization	Name of Subservice Organization(s) and Method of Presentation	Service Provided by the Subservice Organization(s)	Are Complementary User Entity Controls or Complementary Subservice Organization Controls Required by the Service Organization?	Format of the Type 2 Report
1. XYZ Service Organization	Defined contribution recordkeeping system	N/A	N/A	Service organization requires complementary user entity controls	Narrative containing five report components referred to as sections 1, 2, 3, 4, and 5 ²
2. Example Service Organization	Defined contribution recordkeeping system	Computer Subservice Organization Carve-out method	Hosting services	Service organization requires complementary user entity controls and complementary subservice organization controls	Narrative containing five report components referred to as sections 1, 2, 3, 4, and 5 ³

Example 1: Service Organization Requires Complementary User Entity Controls

Report on XYZ Service Organization's Description of its Defined Contribution Recordkeeping System and on the Suitability of the Design and Operating Effectiveness of Its Controls

In example 1, XYZ Service Organization informs report users that complementary user entity controls are required to achieve specific control objectives. Changes to this type 2 report related to the need for complementary user entity controls are shown in boldface italics. This type 2 report includes the following five sections:

² Section 5, "Other Information Provided by XYZ Service Organization," of this type 2 report includes other information not covered by the service auditor's report.

³ Section 5 of this type 2 report includes other information provided by Example Service Organization that is not covered by the service auditor's report.

- Section 1: The independent service auditor's report
- Section 2: Management of XYZ Service Organization's assertion
- Section 3: Management of XYZ Service Organization's description of its system
- Section 4: The service auditor's description of tests of controls and results
- Section 5: Other information provided by XYZ Service Organization

Table of Contents

<u>Section Number</u>	<u>Title of Section</u>
1	Independent Service Auditor's Report
2	XYZ Service Organization's Assertion
3	Description of XYZ Service Organization's Defined Contribution Recordkeeping System Overview of XYZ Service Organization Scope of the Description Internal Control Framework Control Environment Risk Assessment Process Monitoring Activities Information and Communications Control Activities Defined Contribution Plan Setup Control Objectives and Related Controls ⁴ <i>Complementary User Entity Controls</i>
4	Description of XYZ Service Organization's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results

⁴ In this illustrative type 2 report, the control objectives and related controls are included in section 4, "Description of XYZ Service Organization's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results." This avoids the need to repeat the control objectives and related controls in two sections.

5	Other Information Provided by XYZ Service Organization

Section 1: Independent Service Auditor's Report

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's description of its defined contribution recordkeeping system entitled "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) and the suitability of the design and the operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "XYZ Service Organization's Assertion" (assertion). The controls and control objectives included in the description are those that management of XYZ Service Organization believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the defined contribution recordkeeping system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in section 5, "Other Information Provided by XYZ Service Organization," is presented by management of XYZ Service Organization to provide additional information and is not a part of XYZ Service Organization's description of its defined contribution recordkeeping system made available to user entities during the period January 1, 201X, to December 31, 201X. Information about XYZ Service Organization's business continuity planning and management's response to exceptions identified in the report has not been subjected to the procedures applied in the examination of the description of the defined contribution recordkeeping system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the defined contribution recordkeeping system and, accordingly, we express no opinion on it.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, XYZ Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization is responsible for preparing the description and its assertion, including the

completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 201X, to December 31, 201X. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or

conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in XYZ Service Organization's assertion

- a. the description fairly presents the defined contribution recordkeeping system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X.
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 201X, to December 31, 201X, ***and user entities applied the complementary user entity controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.***
- c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 201X, to December 31, 201X, ***if complementary user entity controls assumed in the design of XYZ Service Organization's controls operated effectively throughout the period January 1, 201X, to December 31, 201X.***

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of XYZ Service Organization, user entities of XYZ Service Organization's defined contribution recordkeeping system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Section 2: XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's defined contribution recordkeeping system entitled "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the defined contribution recordkeeping system made available to user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,
 - (1) the types of services provided including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the system captures and addresses significant events and conditions other

than transactions.

- (5) the process used to prepare reports and other information for user entities.
 - (6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.
 - (7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- ii. includes relevant details of changes to the service organization's system during the period covered by the description.
 - iii. 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 user entities of the system and their user auditors, and may not, therefore, include every aspect of the defined contribution recordkeeping system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives *if user entities applied the complementary user entity controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X*. The criteria we used in making this assertion were that
- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
 - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3: Description of XYZ Service Organization's Defined Contribution Recordkeeping System

Overview of XYZ Service Organization

XYZ Service Organization is located in Los Angeles, California, and provides defined contribution plan recordkeeping services to corporations, unions, and nonprofit customers (user entities) across the U.S. These services are provided using a proprietary ABC Recordkeeping application developed and maintained by XYZ Service Organization.

Services provided as part of its defined contribution plan recordkeeping services include the following:

- Benefit plan setup and maintenance
-
-

Scope of the Description

This description addresses only XYZ Service Organization's defined contribution recordkeeping system provided to user entities and excludes other services provided by XYZ Service Organization. The description is intended to provide information for user entities of the defined contribution recordkeeping system and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting, to be used in obtaining an understanding of the defined contribution recordkeeping system and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of XYZ Service Organization's defined contribution recordkeeping system.

Internal Control Framework

This section provides information about the five interrelated components of internal control at XYZ Service Organization, including XYZ Service Organization's

- control environment,
- risk assessment process,
- monitoring activities,
- information and communications, and
- control activities.

Control Environment

The control environment sets the tone of an organization, influencing the control awareness of the organization. The control environment is embodied by the organization's awareness of the

need for controls and the emphasis given to the appropriate controls through management's actions supported by its policies, procedures, and organizational structure.

The following are the primary elements of the service organization's control environment:

1. Commitment to integrity and ethical values
2. Oversight responsibility of the board of directors
3. Assignment of authority and responsibility
4. Commitment to competence
5. Accountability

Commitment to Integrity and Ethical Values

The service organization operates in a highly regulated environment. To this end, the service organization has developed a formal code of ethics available on its intranet that contains rules about employee conduct while under the employ of XYZ Service Organization. Employees are required to read and evidence their knowledge and receipt of the service organization's code of ethics upon hire and annually thereafter.

The service organization offers its employees a number of channels through which potential breaches of ethical behavior may be reported. These channels include....

Oversight Responsibility of the Board of Directors

The control environment at XYZ Service Organization originates with and is the responsibility of the board of directors (board), chief executive officer (CEO), and executive management. The board provides oversight of XYZ Service Organization operations and activities including oversight of the service organization's investment and audit committees. The investment committee supervises and controls the service organization's investment and related financial matters, approves service organization investment policies and guidelines, and reviews the service organization's investment strategies and investment performance. The audit committee is responsible for reviewing the service organization's policies and practices related to accounting, financial, and operational controls, and financial reporting. The audit committee is also responsible for directing the activities of XYZ Service Organization's internal audit department and coordinating the activities of the service organization's external financial auditors.

The internal audit department performs internal audits that help the service organization maintain an effective system of internal control, manage risk, improve customer service, and enhance business performance. The internal audit department follows a risk-based audit approach including

In addition to the internal audit department, the service organization has established several other compliance groups dedicated to effective risk management and oversight, including

Assignment of Authority and Responsibility

Executive management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures, under the ultimate oversight of the board. Management recognizes its responsibility for establishing and maintaining sound internal control and promoting integrity and ethical values to all personnel on a day-to-day basis.

.....

Commitment to Competence

The service organization's commitment to employee competence begins with background checks for all employee candidates and formal hiring practices designed to ensure that new employees are qualified for their job responsibilities. Management has established written competence and performance levels for each job function, including formal promotion and development criteria that help foster professional development for its employees. These criteria are also used to measure employee performance and identify areas for improvement and additional training.

The service organization follows regulatory rules concerning the licensing of personnel in the securities business. Compliance teams monitor license renewals and send update reminders to employees and their supervisors regarding license renewal dates.

The service organization also offers a comprehensive training program including

Accountability

XYZ Service Organization's commitment to an effective system of internal control begins with the service organization's board and its audit committee. The audit committee meets four times a year to fulfill its oversight responsibilities related to the financial reporting process, the system of internal control, internal and external audit activities, and the service organization's process for managing risk and monitoring compliance with applicable laws, regulations, and internal policies and procedures.

The service organization's executive committee meets periodically to oversee critical business operations. In addition ...

Risk Assessment Process

The service organization operates in an environment faced with a variety of risks from internal and external sources.

Objectives

The service organization's risk assessment approach involves an iterative process for identifying and assessing risks to the achievement of the service organization's objectives. This approach forms the basis for determining how risks will be managed by the service organization.

Identification and Analysis of Risks

Risk management is primarily the responsibility of individual business units, which perform periodic risk assessments that identify and document the significant risks facing the service

organization, including any fraud risks. The results of these risk assessments determine how the business units develop and implement controls, operating procedures, and compliance processes for addressing and mitigating such risks. Service organization policies require that any instances of suspected or actual fraud be brought to the immediate attention of senior management, the internal audit department, and the service organization's legal department. In addition ...

Monitoring Activities

XYZ Service Organization employs a combination of ongoing and periodic monitoring activities to monitor that controls are functioning effectively and that risks are appropriately mitigated.

Ongoing Monitoring

The service organization uses a variety of reports and monitoring mechanisms to help ensure that controls are functioning as intended; these include

- electronic display of pending transactions and their status,
- deficiency and incident reporting,
- suspense account reporting,
- daily pricing variances,
- financial reconciliations,
- quality review results and reporting,
- system processing monitoring and reporting, and
- logical security incident logging and review.

Management regularly reviews and assesses business operations to determine that reporting and monitoring mechanisms are used and effective in managing the operations of the business, controls, and related risks.

Periodic Assessments and Monitoring

In addition to ongoing monitoring activities described above, each business unit conducts specific evaluations of risks and controls to maximize the effectiveness of its operations.

The internal audit department performs internal audits of operations and controls to assess the effectiveness of controls. The results of audits and any identified deficiencies are reported to management as well as the audit committee. Management prepares and implements corrective measures to address any significant deficiencies.

Information and Communications

XYZ Service Organization communicates its policies and procedures and other information necessary to help achieve the service organization's business objectives through several means, including the service organization's intranet, emails, newsletters, memoranda, meetings, and training sessions. The service organization's policies and procedures enforce the importance of adherence to and compliance with rules and regulations that govern its business and operations.

XYZ Service Organization has also implemented various methods of communication to inform user entities of the role and responsibilities of XYZ Service Organization in processing their transactions and to communicate significant events to user entities in a timely manner. These methods include XYZ Service Organization's active participation in quarterly user group meetings; the monthly XYZ Service Organization newsletter, which summarizes the significant events and changes during the month and planned for the following month; and the user liaison, who maintains contact with designated user entity representatives to inform them of new issues and developments. User entities are also encouraged to communicate questions and problems to their liaison, and such matters are logged and tracked until resolved, with the resolution also reported to the user entity.

For information provided to user entities, such as reports, statements, data, and other information provided to user entities, service organization policies and procedures require that all such information be tested to ensure it is sufficiently complete and accurate.

Information Systems Overview

The service organization employs the following IT applications and hardware to provide its defined plan contribution recordkeeping services to its user entities:

1. ABC Recordkeeping Application—This system...
2.
3.

*[Note to readers: Paragraph **Error! Reference source not found.** of this guide indicates that the description of the service organization's system may be presented using various formats such as narratives, flowcharts, tables, or graphics, or a combination thereof. For illustrative purposes, this description would include a flowchart.]*

The following flowchart provides an overview of transaction processing for the defined contribution recordkeeping system.

[Note to readers: The flowchart would be inserted here.]

Control Activities

The service organization has developed a variety of policies and procedures including related control activities to help ensure the service organization's objectives are carried out and risks are mitigated. These control activities help ensure that defined contribution plans are administered in accordance with the service organization's policies and procedures.

Control activities are performed at a variety of levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls, including authorizations, reconciliation, and IT controls. Duties and responsibilities—such as duties related to the processing and recording of transactions, investment trading, reconciliation activities, application development, compliance, and control monitoring—are allocated among personnel to ensure that a proper segregation of duties is maintained.

A formal program is in place to review and update the service organization’s policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to employees.

Defined Contribution Plan Setup

Plan Setup

The new accounts team works with plan sponsors, prior recordkeeping service providers, and third-party administrators to facilitate the setup and conversion of the plan in the ABC Recordkeeping application. After receipt of a signed and authorized administrative services agreement from the plan sponsor, a member of the service organization’s new accounts team begins the process of preparing the file for upload into the ABC Recordkeeping application. The new accounts team member uses a new accounts setup checklist to ensure that the plan is completely and accurately set up in the ABC Recordkeeping application. Once the plan is ready for upload, a new accounts team manager reviews the checklist and related documentation to determine whether the plan is completely and accurately set up in the ABC Recordkeeping application and ready for upload. The new accounts team manager signs the checklist as evidence of approval.

After the plan has been set up in the system, the new accounts team manager compares the date the plan was implemented in the system to the date in the administrative service agreement to ensure that the plan was implemented timely. The new accounts team manager also reconciles the dollar total of the plan entered in the system to the dollar total provided by the plan sponsor or prior recordkeeper. Any differences are investigated and resolved. The new accounts team manager completes the checklist to evidence that the reconciliation was performed and that the dollar totals were reconciled.

After the plan has been set up in the ABC Recordkeeping application, a second new accounts team manager reviews the plan information entered in the ABC Recordkeeping application and compares that information to the information in the supporting document provided by the plan sponsor or prior recordkeeper to ensure that the plan was completely and accurately set up in the system. The second new accounts team manager also completes the checklist to evidence that the dollar totals were reconciled and signs the checklist to evidence that the review was performed.

Plan Conversions

For plans set up on the ABC Recordkeeping application from prior recordkeepers, the new accounts team works with...

Plan Changes

For any changes to plans already set up on the ABC Recordkeeping application, the

[Note to readers: For brevity, the following aspects of the defined contribution recordkeeping system are not presented in this illustrative type 2 report.]

Plan administration

Participant administration

Transfers and changes in investment allocation

Contributions and loan payments

Plan distributions and payments

Loan requests

Fees

Investment income

New fund setup and changes

Asset purchases and redemption

Plan and participant statement reporting

Reconciliations

System development and change management

Logical security

Network infrastructure

Computer operations

Data transmission

Physical security

Data backup

Control Objectives and Related Controls

XYZ Service Organization has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in section 4, “Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results,” and are an integral component of XYZ Service Organization’s description of its defined contribution recordkeeping system.

Complementary User Entity Controls

XYZ Service Organization’s controls related to the defined contribution recordkeeping system cover only a portion of overall internal control for each user entity of XYZ Service Organization. It is not feasible for the control objectives related to recordkeeping services to be achieved solely by XYZ Service Organization. Therefore, each user entity’s internal control over financial reporting should be evaluated in conjunction with XYZ Service Organization’s controls and the related tests and results described in section 4 of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable.⁵ In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

Section 4: Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities, is intended to assist auditors in planning the audit of user entities’ financial statements or user entities’ internal control over financial reporting and in assessing control risk for assertions in user entities’ financial statements that may be affected by controls at XYZ Service Organization.

Our examination was limited to the control objectives and related controls specified by XYZ Service Organization in sections 3 and 4 of the report, and did not extend to controls in effect at user entities.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess total internal control. If internal control is not effective at user entities, XYZ Service Organization’s controls may not compensate for such weaknesses.

⁵ There is no prescribed format for presenting the complementary user entity controls. They may be listed in section 4 following the service organization’s description of control objectives and related controls, and the service auditor’s description of tests of controls and results, to which they apply, or they may be listed in the description of the service organization’s system in section 3. If listed in section 3, the complementary user entity controls should identify the control objectives to which they apply.

XYZ Service Organization’s internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by XYZ Service Organization. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by XYZ Service Organization, we considered aspects of XYZ Service Organization’s control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Test	Description
Inquiry	Inquiry of appropriate personnel and corroboration with management
Observation	Observation of the application, performance, or existence of the control
Inspection	Inspection of documents and reports indicating performance of the control
Reperformance	Reperformance of the control

In addition, as required by paragraph .35 of AT-C section 205 and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Control Objective 1—Defined Contribution Plan Setup

Controls provide reasonable assurance that defined contribution plans set up on the ABC Recordkeeping application are authorized by plan sponsors and completely and accurately processed and recorded in a timely manner.⁶

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
1.1 New plans or plans from prior recordkeepers are accepted and entered in the ABC Recordkeeping application only after receipt of a signed and authorized administrative services agreement from the plan sponsor. A member of the service organization’s	For a sample of new plans, <ul style="list-style-type: none"> inspected the administrative services agreement to determine whether the agreement was signed and authorized by the plan sponsor. inspected the new accounts setup checklist to determine whether the 	No exceptions noted.

⁶ For illustrative purposes the phrase “in a timely manner” is used in this control objective. However, in order for the control objective to be measurable, the service organization would need to define “in a timely manner,” for example, “the transaction was entered in the ABC Recordkeeping application within 10 business days of receipt.”

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<p>new accounts team uses a new accounts setup checklist to ensure that plans are</p> <ul style="list-style-type: none"> • set up completely and accurately in the ABC Recordkeeping application, based on the information in the supporting document provided by the plan sponsor or prior recordkeeper. • set up and implemented by the date specified in the administrative services agreement. <p>A new accounts team manager is assigned to the plan and signs the checklist to evidence that the plan was completely and accurately set up and implemented by the date specified in the administrative services agreement.</p>	<p>checklist was completed and signed by the new accounts team manager.</p> <ul style="list-style-type: none"> • ... 	
<p>1.2 After the plan is set up in the ABC Recordkeeping application, the new accounts team manager compares the plan information entered in the ABC Recordkeeping application to the information in the related administrative services agreement and supporting document provided by the plan sponsor or prior recordkeeper to ensure that the plan was completely and accurately set up and implemented by the date specified in the administrative services agreement.</p>	<p>For a sample of new plans set up in the ABC Recordkeeping application,</p> <ul style="list-style-type: none"> • inspected the related administrative services agreement to determine whether the implementation date per the ABC Recordkeeping application was no later than the implementation date per the administrative services agreement. • reperformed the control by comparing the plan information entered in the ABC Recordkeeping application to the plan information included in the supporting document provided by the plan sponsor or prior recordkeeper to ensure that the plan was completely and accurately set up. 	<p>No exceptions noted.</p>
<p>1.3 After the plan is set up in the ABC Recordkeeping application, the new accounts team manager reconciles the total plan dollars entered in the ABC Recordkeeping application to the total plan dollars per the supporting document provided by the plan sponsor or prior recordkeeper and includes</p>	<p>For a sample of new plans set up in the ABC Recordkeeping application, inspected the checklist to determine whether the new accounts team manager</p> <ul style="list-style-type: none"> • prepared a reconciliation of the total plan dollars entered in the ABC Recordkeeping application to the 	<p>No exceptions noted.</p>

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<p>the reconciliation in the checklist. Any differences are investigated and resolved.</p>	<p>total plan dollars per the supporting document provided by the plan sponsor or prior recordkeeper.</p> <ul style="list-style-type: none"> investigated and resolved any differences between the two amounts. <p>For a sample of new plans, reperformed the reconciliation of the total plan dollars entered in the ABC Recordkeeping application to the total plan dollars per the supporting document provided by the plan sponsor or prior recordkeeper to determine whether the two amounts reconciled and whether reconciling items had been investigated and resolved.</p>	
<p>1.4 Using the new accounts setup checklist, a second new accounts team manager compares the plan information entered in the ABC Recordkeeping application to the information in the administrative services agreement and supporting document provided by the plan sponsor or prior recordkeeper to ensure that the plan was completely and accurately set up in the ABC Recordkeeping application and implemented by the date specified in the administrative services agreement. The second new accounts team manager also</p> <ul style="list-style-type: none"> reviews the reconciliation of the total plan dollars entered in the ABC Recordkeeping application to the total plan dollars per the supporting document provided by the plan sponsor or prior recordkeeper to ensure that the reconciliation was performed and that the two amounts were reconciled. signs the checklist to evidence that the review was performed. 	<p>For a sample of new plans set up in the ABC Recordkeeping application, inspected the related new accounts setup checklist to determine whether it was signed by a second new accounts team manager.</p>	<p>No exceptions noted.</p>
1.5 ...		
1.6...		
Complementary User Entity Controls		
1. Plan sponsors are responsible for ensuring that plan information provided to XYZ Service Organization is complete		

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<p><i>and accurate and provided on a timely basis.</i></p> <p>2. <i>Plan sponsors are responsible for ensuring that administrative agreements are signed by authorized plan sponsor personnel and provided to XYZ Service Organization.</i></p> <p>3. <i>Plan sponsors are responsible for ensuring that any changes to plans already set up in the ABC Recordkeeping application are sent to XYZ Service Organization from authorized personnel on a timely basis and that such changes are complete and accurate.</i></p> <p>4. ...</p>		

Control Objective 2—Plan Administration

Controls provide reasonable assurance that changes to plan data are authorized and are processed and recorded in an accurate, complete, and timely manner.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<p>2.1 For changes to plans set up in the ABC Recordkeeping application and originating from plan sponsors, a member of the service organization's account changes team verifies that the change was received from a person authorized by the plan sponsor, updates the plan information in the ABC Recordkeeping application based on the document requesting the change, and completes and signs the account changes checklist to ensure that the change was accurately entered in the ABC Recordkeeping application.</p> <p>Using the account change checklist, a second member of the account changes team reviews the change entered in the ABC Recordkeeping application and compares it to the information in the document requesting the change to ensure that the change was accurately entered no later than 10 business days after the receipt of the change request. The second member of the account changes team signs the checklist to evidence that the review was performed.</p>	<p>For a sample of plan changes originating from plan sponsors and entered in the ABC Recordkeeping application,</p> <ul style="list-style-type: none"> inspected the documents requesting the change and the account changes checklist to determine whether the change was authorized by a person authorized by the plan sponsor and the checklist was completed and signed by a member of the account changes team. reperformed the control by comparing the change made to the plan in the ABC Recordkeeping application to the document from the plan sponsor requesting the change to determine whether the change was entered accurately in the ABC Recordkeeping application no later than 10 business days after the receipt of the change request. inspected the account changes checklist to determine whether the second member of the account changes team signed the checklist. 	<p>No exceptions noted.</p>

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
2.2...		
2.3...		
Complementary User Entity Controls		
<ol style="list-style-type: none"> 1. <i>Plan sponsors are responsible for submitting complete and accurate plan changes to XYZ Service Organization on a timely basis.</i> 2. <i>Plan sponsors are responsible for verifying any changes to their respective account or plan information and notifying XYZ Service Organization of any errors or discrepancies on a timely basis.</i> 3. ... 4. ... 		

Control Objective 3—Participant Administration

Controls provide reasonable assurance that participant enrollments and changes to participant data are authorized and completely and accurately processed and recorded in a timely manner.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<p>3.1 Participant enrollment forms or participant change requests received via mail, email, or fax are logged and reviewed by an account processing specialist for completeness, authorization (a signature on or accompanying the form), and accuracy prior to entering the information in the ABC Recordkeeping application. Service organization policy requires that all information in the participant enrollment form or change request be completely and accurately entered in the ABC Recordkeeping system within 10 business days of receipt. After entry of the information in the ABC Recordkeeping application and prior to production implementation, the account processing specialist signs the participant enrollment form or change request and forwards the form or request to a second account processing specialist for review.</p> <p>The second account processing specialist</p>	<p>For a sample of participant enrollment forms and participant change requests, inspected</p> <ul style="list-style-type: none"> • the log to determine whether the form or change request was logged. • the participant enrollment form or change request to determine whether it was signed by <ul style="list-style-type: none"> – an account processing specialist to evidence that the form or change request was reviewed for completeness, authorization, and accuracy prior to entry in the ABC Recordkeeping application. – a second account processing specialist to evidence that the specialist compared the information entered in the ABC Recordkeeping application with the 	<p>No exceptions noted.</p>

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<ul style="list-style-type: none"> • compares the information entered in the ABC Recordkeeping application with the information in the participant enrollment form or change request to ensure that the information was entered accurately and completely within 10 business days of receipt. • resolves any differences and indicates on the participant enrollment form or change request any changes that need to be made to the information previously entered in the ABC Recordkeeping application. • if applicable, sends the participant enrollment form or change request back to the first account processing specialist with instructions for correcting the information in the ABC Recordkeeping application. • signs the participant enrollment or change request to evidence that the review and related procedures were performed. 	<p>information in the participant enrollment form or change request to ensure that the information was entered completely and accurately within 10 business days of receipt of complete and accurate data.</p> <p>For a sample of participant enrollment forms and change requests received via mail, email, or fax, reperformed the control by comparing the participant enrollment or change information in the ABC Recordkeeping application to the information in the participant enrollment form or change request submitted by the participant or plan sponsor to determine whether the information in the application was entered completely and accurately within 10 business days of receipt.</p>	
<p>3.2 For participant enrollment requests received electronically, the plan sponsor must sign on to the XYZ Service Organization plan sponsor web portal and submit the electronic file of participant enrollment information. Plan sponsors are required to authenticate themselves to the web portal via a valid user ID and password. Files uploaded via the XYZ Service Organization web portal are uploaded via file transfer protocol (FTP) or secure FTP.</p>	<p>Inspected the configuration of logical security over the web portal to determine whether authentication to the portal requires a valid user ID and password.</p> <p>For a sample of dates, inspected the FTP or secure FTP configuration for transfer or upload of files to the web portal to determine whether FTP is required.</p>	<p>No exceptions noted.</p>

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
3.3 For plans that enroll participants electronically, participants are identified in a data file that is transmitted by upload of the file to the XYZ Service Organization web portal. Participants are added to the ABC Recordkeeping application based on plan eligibility requirements and plan parameters. After upload of the file, validation routines are run against the file to identify any errors or incomplete information. Any errors or incomplete participant information that is not corrected is returned to the plan sponsor for correction.	<p>For a sample of participant data files received via electronic file upload,</p> <ul style="list-style-type: none"> inspected the participant information in the ABC Recordkeeping application to determine whether the information was completely and accurately loaded into the application. inspected whether validation routines were run to identify any errors or incomplete data and whether any remaining errors or incomplete data were returned to the plan sponsor for correction. 	No exceptions noted.
3.4 Participant access to the voice response system, the participant web portal, and the XYZ Service Organization call center requires entry of a valid personal identification number (PIN).	Observed that access to the voice response system, the participant web portal, and the call center requires entry of a valid PIN.	No exceptions noted.
3.5 For participant changes received via the call center, the automated telephone voice response system, or participant web portal, a change notification is generated and mailed to the participant.	For a selection of participant changes received via the call center, automated telephone voice response system, or participant web portal, inspected the related notification sent to the participant to determine that the notification accurately reflects the change made to the participant's information.	No exceptions noted.
3.6 ...		
3.7 ...		
Complementary User Entity Controls		
<ol style="list-style-type: none"> <i>Plan sponsors are responsible for submitting complete and accurate employee enrollment information to XYZ Service Organization on a timely basis.</i> <i>Plan sponsors and participants are responsible for submitting complete and accurate participant change information to XYZ Service Organization on a timely basis.</i> <i>Plan sponsors and participants are responsible for verifying any changes to the respective participant account information and notifying the XYZ Service Organization of any errors or discrepancies on a timely basis.</i> 		

[Note to readers: For brevity, the controls and test of controls and results for control objectives 4–13 are not presented in this illustrative report.]

Control Objective 4—Transfers and Changes in Investment Allocations

Controls provide reasonable assurance that participant-initiated transfers and changes in investment allocations are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 5—Contributions and Loan Payments

Controls provide reasonable assurance that contributions and loan payments are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 6—Plan Distributions and Payments

Controls provide reasonable assurance that plan distributions and payments to participants are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 7—Loan Requests

Controls provide reasonable assurance that loan requests are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 8—Fees

Controls provide reasonable assurance that requests for new fee setup, changes, corrections, terminations, and reversals are completely and accurately processed and recorded in the ABC Recordkeeping application in a timely manner.

Control Objective 9—Investment Income

Controls provide reasonable assurance that investment income, dividends, corporate actions, and participant account values are completely and accurately calculated, processed, and recorded in a timely manner.

Control Objective 10—New Fund Setup and Changes

Controls provide reasonable assurance that new funds and changes to funds are authorized and completely and accurately implemented in a timely manner.

Control Objective 11—Asset Purchases and Redemption

Controls provide reasonable assurance that asset purchase and redemption transactions are authorized and completely and accurately traded and recorded in a timely manner.

Control Objective 12—Plan and Participant Statement Reporting

Controls provide reasonable assurance that plan and participant statements are accurate, complete, and provided to or sent to the plan sponsors or participants in a timely manner, in accordance with contractual agreements.

Control Objective 13—Reconciliations

Controls provide reasonable assurance that cash and security positions are completely and accurately reconciled between the ABC Recordkeeping application and the depositories in a timely manner.

Control Objective 14—Systems Development and Change Management
Controls provide reasonable assurance that changes to the ABC Recordkeeping application, other programs, and related data management systems are authorized, tested, documented, approved, and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities’ financial reporting and to support user entities’ internal control over financial reporting.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
14.1 The service organization has established written policies and procedures for systems development and change management.	Inspected the service organization’s systems development and change management policies and procedures to determine whether written policies and procedures have been established.	No exceptions noted.
14.2 Requests for new development or changes to existing applications must be documented in a change request form and approved by the business owner (as appropriate) and IT management.	For a sample of new development or changes to existing applications, inspected the change request form to determine whether the request was approved by the business owner and IT management.	No exceptions noted.
14.3 For large projects, change requests are assigned to a system analyst to assess and document the nature and extent of the work and number of project hours required to complete the task. IT management must approve such change requests and indicate approval on the change request form.	For a sample of large projects, inspected the change request form for evidence that a system analyst had assessed and documented the nature and extent of the work and number of project hours required to complete the task, and that the change request form was approved by IT management.	No exceptions noted.
14.4 Upon completion of development, the completed code is tested by the quality assurance department in the test environment. Approval by the quality assurance department is documented on the change request form.	For a sample of program changes implemented into production, inspected the change request form to determine whether testing was performed and approved by the quality assurance department.	No exceptions noted.
14.5 Upon approval by the quality assurance department, the change request form is forwarded to the change control board for approval. Approval by the change control board is documented on the change request form.	For a sample of program changes implemented into production, inspected the change request form to determine whether the request was approved by the change control board.	No exceptions noted.
14.6 All changes approved for production implementation are moved to the staging environment and implemented into production by the IT configuration group. When this occurs the change control board team member	For a sample of program changes implemented into production, inspected the change request form to determine whether the change was moved to the staging environment and implemented into production by the IT configuration	No exceptions noted.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
notes this on the checklist	group.	
14.7 Separate environments exist for the development, testing, staging, and production of changes.	Inspected the URLs to determine whether separate environments exist for the development, testing, staging, and production of changes.	No exceptions noted.
14.8 Change control software is used to implement changes into production and to maintain version control over program source code. Any changes to the production code are logged by the software.	Inspected the change control software and related logs to determine whether change control software is used to implement changes into production, maintain version control over program source code, and log changes to the production code.	No exceptions noted.
14.9 Access to the production environment and the change control software is restricted to authorized IT configuration personnel.	On multiple occasions during the period, inspected the security permissions for the change control software and production environment to determine whether access to implement changes into production is restricted to authorized IT configuration personnel.	No exceptions noted.
14.10 ...		
14.11 ...		

Control Objective 15—Logical Security

Controls provide reasonable assurance that logical access to programs, data, the ABC Recordkeeping application, and computer resources that may affect user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
15.1 The service organization has established formal policies and procedures related to logical security and controls over access to and use of service organization applications.	Inspected the service organization's IT security policies and procedures to determine whether formal policies and procedures have been established.	No exceptions noted.
15.2 Requests for new user access to the service organization's system are initiated by the human resources department and the employee's hiring manager by completing an online system access form. The form is forwarded to the IT security group for setup of user access to the service	For a selection of new employee hires, inspected the employee's associated ABC Recordkeeping application access form and the level of access granted to the employee to determine whether the user's access was properly approved and provisioned and that the level of access granted was commensurate with	No exceptions noted.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
organization's system. User entities are assigned access rights in the ABC Recordkeeping application based on job responsibilities, and security groups are used in the system to segregate and restrict user access.	the user's job responsibilities.	
15.3 System administrator access to the network and ABC Recordkeeping application is restricted to authorized personnel.	Inspected the list of users with administrative access to the network and the ABC Recordkeeping application and reviewed the list with IT management to determine whether administrative access is appropriately restricted to authorized personnel.	No exceptions noted.
15.4 The access of terminated employees is removed or disabled by the IT security group based on notification from the human resources department. The human resources department completes a ticket in the help desk ticketing system that requests the removal of the employee's system access on a specific date.	For a selection of terminated employees, inspected the employee's access to the network and ABC Recordkeeping application to determine whether the employee's access was properly removed or disabled on or before the date specified by the human resources department.	For 1 out of 25 terminated employees selected for testing, the employee's access to the ABC Recordkeeping application was not removed from the system.
15.5 User access to the network and ABC Recordkeeping application is reviewed twice a year for appropriateness by the IT security group and the application owner. Any access deemed inappropriate is removed or modified by the IT security group.	Inspected a selection of semi-annual user access reviews performed by the IT security group and the application owner to determine whether user access was reviewed for appropriateness and whether the access of any user with inappropriate access was removed or modified.	No exceptions noted.
15.6 Access to the network and ABC Recordkeeping application requires a valid user ID and password.	Inspected the security configuration of the network and application on multiple occasions during the period and observed the login process to determine that a valid user ID and password are required to authenticate the user.	No exceptions noted.
15.7 Password security parameters for the network have been established for the following areas in accordance with service organization policy: <i>Network</i> <ul style="list-style-type: none"> • Minimum password length • Password complexity • Minimum password age • Password history 	Inspected the security configuration of the network and ABC Recordkeeping application to determine whether parameters have been configured for the specified areas in accordance with service organization policy.	No exceptions noted.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<ul style="list-style-type: none"> Number of invalid login attempts <i>ABC Recordkeeping Application</i> <ul style="list-style-type: none"> Minimum password length Password complexity Minimum password age Password history Number of invalid login attempts 		
15.8 Direct access to the ABC Recordkeeping application database is restricted to authorized personnel. Administrators are required to “SU” to root ⁷ to obtain root privileges.	For a sample of administrators with access to the ABC Recordkeeping application database, inspected the related security configuration to determine whether direct access is restricted to authorized personnel and whether administrators are required to SU to root.	No exceptions noted.
15.9 Firewalls are implemented on the network to filter traffic and protect the network from external threats and vulnerabilities.	Inspected the configuration of the firewall to determine whether access rulesets are configured to filter traffic and to protect the network.	No exceptions noted.
15.10 Access to the firewall requires a user ID and password with access to the firewall ruleset ⁸ and configuration restricted to authorized IT personnel.	Observed that access to the firewall requires a user ID and password. Inspected the firewall configuration to determine whether administrative access is restricted to authorized IT personnel.	No exceptions noted.
15.11 A Point-to-Point Tunneling Protocol (PPTP) based virtual private network (VPN) is used to provide employees with remote access to the internal network. The VPN uses Windows active directory authentication and Microsoft PPTP 128-bit encryption.	Inspected the PPTP-based VPN configuration to determine whether remote user access is controlled via VPN technology and whether Windows authentication and 128-bit encryption is used to access the network.	No exceptions noted.
15.12 Antivirus software is installed on all servers and workstations to protect against viruses and malware. Antivirus software is configured to download virus definition updates every 90 minutes.	Inspected the configuration of the antivirus software to determine whether it is installed on servers and workstations and whether it is configured to receive virus updates every 90 minutes.	No exceptions noted.
<i>Complementary User Entity Controls</i>		
<i>1. Plan sponsors are responsible for ensuring that logical access to ABC Recordkeeping application for their personnel</i>		

⁷ *SU to root* is a way by which privileged access is assigned to a user ID.

⁸ *Firewall ruleset* are the rules that govern what the firewall will allow or disallow.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
<i>is appropriate based on job responsibility.</i>		
2. ...		
3. ...		

Control Objective 16—Computer Operations

Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner, with respect to user entities' internal control over financial reporting.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
16.1 All computer jobs are scheduled using job scheduling software.	Inspected the job processing software to determine whether computer jobs are processed using job scheduling software.	No exceptions noted.
16.2 Access to the job scheduling software is restricted to authorized IT personnel. Any changes to job schedules must be approved by the vice president of IT operations.	<p>Inspected the configuration of security over the job scheduling software to determine whether access is restricted to authorized personnel.</p> <p>Inspected the job scheduler to determine whether computer jobs were changed during the examination period.</p>	<p>No exceptions noted.</p> <p>The operating effectiveness of the control related to approval of changes to job schedules could not be tested because no changes were made to computer jobs during the examination period.</p>
16.3 The job processing software logs the processing of all computer jobs and provides status alerts of job completions and failures.	For a selection of completed and failed computer jobs, inspected the computer logs to determine whether the jobs were logged and whether status alerts were produced.	No exceptions noted.
16.4 Job processing is monitored by IT operations personnel using the job scheduling software. Any job errors or deviations from scheduled processing are resolved as appropriate.	On multiple occasions during the period, observed IT operations personnel monitoring computer jobs and the actions taken to resolve processing errors.	No exceptions noted.
16.5...		

[Note to readers: For brevity, the controls and tests of controls and results for control objectives 17–20 are not presented in this illustrative report.]

Control Objective 17—Network Infrastructure

Controls provide reasonable assurance that network infrastructure is configured as authorized, with respect to user entities' internal control over financial reporting, to support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances and to protect data from unauthorized changes.

Control Objective 18—Data Transmissions

Controls provide reasonable assurance that data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely, with respect to user entities' internal control over financial reporting.

Control Objective 19—Physical Security

Controls provide reasonable assurance that physical access to computer and other resources, with respect to user entities' internal control over financial reporting, is restricted to authorized and appropriate personnel.

Control Objective 20—Data Backup

Controls provide reasonable assurance that data and systems are backed up regularly and available for restoration in the event of processing errors or unexpected processing interruptions, with respect to user entities' internal control over financial reporting.

Section 5: Other Information Provided by XYZ Service Organization

- Business Continuity Planning
- ...
- Management's Response to Exceptions Identified
- ...

Example 2 : Service Organization Uses Carve-Out Method for Subservice Organization; Service Organization Requires Complementary User Entity Controls and Complementary Subservice Organization Controls

Example Service Organization

Report on Example Service Organization's Description of Its Defined Contribution Recordkeeping System and on the Suitability of the Design and Operating Effectiveness of Its Controls

In example 2, Example Service Organization outsources aspects of its computer processing to a subservice organization, Computer Subservice Organization, and elects to use the carve-out method of presentation. In addition, complementary user entity and complementary subservice organization controls are required to achieve certain control objectives. Changes to this type 2 report related to Example Service Organization's use of a subservice organization and the need

for complementary user entity and complementary subservice organization controls are shown in boldface italics. This report is written in narrative format and includes the following five sections:

Section 1: The independent service auditor's report

Section 2: Management of Example Service Organization's assertion

Section 3: Management of Example Service Organization's description of its system

Section 4: The service auditor's description of tests of controls and results

Section 5: Other information provided by Example Service Organization

Table of Contents

Section Number	Title of Section
1	Independent Service Auditor's Report
2	Example Service Organization's Assertion
3	<p>Description of Example Service Organization's Defined Contribution Recordkeeping System</p> <p>Overview of Example Service Organization</p> <p>Scope of the Description</p> <p>Internal Control Framework</p> <p>Control Environment</p> <p>Risk Assessment Process</p> <p>Monitoring Activities</p> <p>Information and Communications</p> <p>Control Activities</p> <p>Defined Contribution Plan Setup</p> <p>Control Objectives and Related Controls⁹</p> <p><i>Complementary Subservice Organization Controls</i></p> <p><i>Complementary User Entity Controls</i></p>
4	Description of Example Service Organization's Control Objectives and Related Controls, and Independent Service Auditor's Description of

⁹ In this illustrative report, the control objectives and related controls are included in section 4, "Description of Example Service Organization's Control Objectives and Related Controls, and Independent Service Auditor's Description of Tests of Controls and Results." This avoids the need to repeat the control objectives and related controls in two sections.

	Tests of Controls and Results
5	Other Information Provided by Example Service Organization

Section 1: Independent Service Auditor's Report

To: Example Service Organization

Scope

We have examined Example Service Organization's description of its defined contribution recordkeeping system entitled "Example Service Organization's Description of its Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Example Service Organization's Assertion" (assertion). The controls and control objectives included in the description are those that management of Example Service Organization believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the defined contribution recordkeeping system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in section 5, "Other Information Provided by Example Service Organization," is presented by management of Example Service Organization to provide additional information and is not a part of Example Service Organization's description of its defined contribution recordkeeping system made available to user entities during the period January 1, 201X, to December 31, 201X. Information about Example Service Organization's business continuity planning and management's response to exceptions identified in the report has not been subjected to the procedures applied in the examination of the description of the defined contribution recordkeeping system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the defined contribution recordkeeping system and, accordingly, we express no opinion on it.

Example Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of Example Service Organization and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Example Service Organization can be achieved only if complementary subservice organization controls assumed in the design of Example Service Organization's controls are suitably designed and operating effectively, along with the related controls at Example Service Organization. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Example Service

Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, Example Service Organization has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Example Service Organization is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 201X, to December 31, 201X. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria referenced above.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives

stated therein, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in Example Service Organization's assertion,

- a. the description fairly presents the defined contribution recordkeeping system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X.
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 201X, to December 31, 201X, ***and the subservice organization and user entities applied the complementary controls assumed in the design of Example Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.***
- c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 201X, to December 31, 201X, ***if complementary subservice organization and user entity controls assumed in the design of Example Service Organization's controls operated effectively throughout the period January 1, 201X, to December 31, 201X.***

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Example Service Organization, user entities of Example Service Organization's defined contribution recordkeeping system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material

misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Section 2: Example Service Organization's Assertion

We have prepared the description of Example Service Organization's defined contribution plan recordkeeping system entitled "Example Service Organization's Description of its Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, ***including information about controls implemented by the subservice organization and user entities of the system themselves***, when assessing the risks of material misstatement of user entities' financial statements.

Example Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of Example Service Organization and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Example Service Organization can be achieved only if complementary subservice organization controls assumed in the design of Example Service Organization's controls are suitably designed and operating effectively, along with the related controls at Example Service Organization. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Example Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the defined contribution recordkeeping system made available to user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

- (1) the types of services provided, including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the system captures and addresses significant events and conditions other than transactions.
 - (5) the process used to prepare reports and other information for user entities.
 - (6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.
 - (7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- ii. includes relevant details of changes to the service organization's system during the period covered by the description.
 - iii. 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 user entities of the system and their user auditors and may not, therefore, include every aspect of the defined contribution recordkeeping system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives ***if the subservice organization and user***

entities applied the complementary controls assumed in the design of Example Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.
The criteria we used in making this assertion were that

- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
- ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
- iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3: Description of Example Service Organization's Defined Contribution Recordkeeping System

Overview of Example Service Organization

Example Service Organization is located in Los Angeles, California, and provides defined contribution plan recordkeeping services to corporations, unions, and nonprofit customers (user entities) across the U.S. These services are provided using a proprietary ABC Recordkeeping application developed and maintained by Example Service Organization.

Services provided as part of its defined contribution plan recordkeeping services include the following:

- Benefit plan setup and maintenance
-
-

Scope of the Description

This description of Example Service Organization's defined contribution recordkeeping system addresses only Example Service Organization's defined contribution recordkeeping system provided to its user entities and excludes other services provided by the Example Service Organization. The description is intended to provide information for user entities of the defined contribution recordkeeping system and their independent auditors who audit and report on such user entities' financial statements to be used in obtaining an understanding of the defined contribution recordkeeping system and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of Example Service Organization's defined contribution recordkeeping system.

Example Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of Example Service Organization and excludes the control objectives and related controls of the subservice organization.

Internal Control Framework

This section provides information about the five interrelated components of internal control at Example Service Organization, including Example Service Organization's

- control environment,
- risk assessment process,
- monitoring activities,
- information and communications, and
- control activities.

[Note to readers: For brevity, and except as noted below for monitoring activities, the internal control framework of Example Service Organization would be the same as that provided in example 1 and is not repeated here.]

Monitoring Activities

Example Service Organization employs a combination of ongoing and periodic monitoring activities to monitor that controls are functioning effectively and that risks are appropriately mitigated.

Ongoing Monitoring

The service organization uses a variety of reports and monitoring mechanisms to help ensure that controls are functioning as intended; these include

- electronic display of pending transactions and their status,
- deficiency and incident reporting,
- suspense account reporting,
- daily pricing variances,
- financial reconciliations,
- quality review results and reporting, and

- system processing monitoring and reporting.

Management regularly reviews and assesses business operations to determine that reporting and monitoring mechanisms are used and effective in managing the operations of the business, controls, and related risks.

Periodic Assessments and Monitoring

In addition to the ongoing monitoring activities described above, each business unit conducts specific evaluations of risks and controls to maximize the effectiveness of its operations.

The internal audit department performs internal audits of operations and controls to assess the effectiveness of controls. The results of audits and any identified deficiencies are reported to management as well as the audit committee. Management prepares and implements corrective measures to address any significant deficiencies.

Monitoring of the Subservice Organization

Example Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services.

Management and the internal audit department of Example Service Organization receive and review the type 2 SOC 1[®] report of Computer Subservice Organization on an annual basis. In addition, through its daily operational activities, management of Example Service Organization monitors the services performed by Computer Subservice Organization to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes planned at the hosting facility, and relay any issues or concerns to subservice organization management.

Defined Contribution Plan Setup

Plan Setup

The new accounts team works with plan sponsors, prior recordkeeping service providers, or third-party administrators to facilitate the setup and conversion of the plan in the ABC Recordkeeping application. After receipt of a signed and authorized administrative services agreement from the plan sponsor, a member of the new accounts team begins the process of preparing the file for upload into the ABC Recordkeeping application. The member of the new accounts team uses a checklist to ensure that plans are completely and accurately set up in the ABC Recordkeeping application. Once the plan is ready for upload, a new accounts team manager approves the file upload and signs the checklist as evidence that the plan was completely and accurately set up in the system.

After the plan has been set up in the system, the new accounts team manager compares the date the plan is to be implemented in the system to the date in the administrative service agreement to ensure that the plan will be implemented timely. The new accounts team manager also reconciles

the dollar total of the plan entered in the system to the dollar total provided by the plan sponsor or prior recordkeeper. Any differences are investigated and resolved. The new accounts team manager completes the checklist to evidence that the reconciliation was performed and that the two dollar totals were reconciled.

After the plan has been set up in the ABC Recordkeeping application, a second new accounts team manager reviews the plan information entered in the ABC Recordkeeping application and compares information entered to plan documents to ensure the plan was completely and accurately set up in the system. The second new accounts team manager also completes the checklist to evidence that the dollar totals were reconciled. The second new accounts team manager signs the checklist to evidence that the review was performed.

[Note to readers: For brevity, the remainder of “Example Service Organization’s Description of Its Defined Contribution Recordkeeping System” is not presented in this illustrative type 2 report.]

Control Objectives and Related Controls

Example Service Organization has specified the control objectives and identified the controls that are designed to achieve the related control objective. The specified control objectives, related controls, and complementary user entity controls are presented in section 4, “Description of Example Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results,” and are an integral component of Example Service Organization’s description of its defined contribution recordkeeping system.

Complementary Subservice Organization Controls (CSOC)

Example Service Organization’s controls related to the defined contribution recordkeeping system cover only a portion of overall internal control for each user entity of Example Service Organization. It is not feasible for the control objectives related to recordkeeping services to be achieved solely by Example Service Organization. Therefore, each user entity’s internal control over financial reporting must be evaluated in conjunction with Example Service Organization’s controls and the related tests and results described in section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	<i>Complementary Subservice Organization Controls (CSOCs)</i>	<i>Related Control Objective</i>
	<i><u>Computer Subservice Organization</u></i>	
<i>1.</i>	<i>Computer Subservice Organization is responsible for maintaining logical security over the servers and other hardware devices upon which the ABC Recordkeeping application is hosted.</i>	<i>CO 15</i>
<i>2.</i>	<i>Computer Subservice Organization is responsible for notifying Example Service Organization of any security incidents related to security over the servers and other hardware devices upon which the ABC Recordkeeping application is hosted.</i>	<i>CO 15</i>
<i>3.</i>	<i>Computer Subservice Organization is responsible for maintaining physical security over its data center in which the servers used to host the ABC Recordkeeping application are housed.</i>	<i>CO 19</i>
<i>4.</i>	<i>.....</i>	

Complementary User Entity Controls

Example Service Organization’s controls related to the defined contribution recordkeeping system cover only a portion of overall internal control for each user entity of Example Service Organization. It is not feasible for the control objectives related to recordkeeping services to be achieved solely by Example Service Organization. Therefore, each user entity’s internal control over financial reporting should be evaluated in conjunction with Example Service Organization’s controls and the related tests and results described in section 4 of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable.¹⁰ In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

Section 4: Description of Example Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

¹⁰ There is no prescribed format for presenting complementary user entity controls. They may be listed in section 4 following the control objectives, tests of controls, and results of tests to which they apply or they may be listed in the description of the service organization’s system in section 3. If listed in section 3, the complementary user entity controls should identify the control objectives to which they apply.

[Note to readers: For brevity, the details of “Information Provided by the Independent Service Auditor” are not presented in this illustrative type 2 report.]

Control Objective 1—Defined Contribution Plan Setup

Controls provide reasonable assurance that defined contribution plans set up on the ABC Recordkeeping application are authorized by plan sponsors and completely and accurately processed and recorded in a timely manner.

Controls Specified by Example Service Organization	Tests of Controls	Results of Tests
<p>1.1 New plans or plans from prior recordkeepers are accepted and entered in the ABC Recordkeeping application only after receipt of a signed and authorized administrative services agreement from the plan sponsor. A member of the service organization’s new accounts team uses a new accounts setup checklist to ensure that plans are</p> <ul style="list-style-type: none"> • set up completely and accurately in the ABC Recordkeeping application, based on the information in the supporting document provided by the plan sponsor or prior recordkeeper. • set up and implemented by the date specified in the administrative services agreement. <p>A new accounts team manager is assigned to the plan and signs the checklist to evidence that the plan was completely and accurately set up and implemented by the date specified in the administrative services agreement.</p>	<p>For a sample of new plans,</p> <ul style="list-style-type: none"> • inspected the administrative services agreement to determine whether the agreement was signed and authorized by the plan sponsor. • inspected the new accounts setup checklist to determine whether the checklist was completed and signed by the new accounts team manager. • ... 	<p>No exceptions noted.</p>
1.2...		

Controls Specified by Example Service Organization	Tests of Controls	Results of Tests
<i>Complementary User Entity Controls</i>		
<ol style="list-style-type: none"> 1. <i>Plan sponsors are responsible for ensuring that plan information provided to Example Service Organization is complete and accurate and provided on a timely basis.</i> 2. <i>Plan sponsors are responsible for ensuring that administrative agreements are signed by authorized plan sponsor personnel and provided to Example Service Organization.</i> 3. <i>Plan sponsors are responsible for ensuring that any changes to plans already set up in the ABC Recordkeeping application are sent to Example Service Organization from authorized personnel on a timely basis and that such changes are complete and accurate.</i> 4. ... 		

[Note to readers: For brevity, Example Service Organization's description of its controls and the independent service auditor's description of tests of controls and results for control objectives 2–20 are not presented in this illustrative type 2 report.]

Control Objective 2—Plan Administration

Controls provide reasonable assurance that changes to plan data are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 3—Participant Administration

Controls provide reasonable assurance that participant enrollments and changes to participant data are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 4—Transfers and Changes in Investment Allocations

Controls provide reasonable assurance that participant-initiated transfers and changes in investment allocations are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 5—Contributions and Loan Payments

Controls provide reasonable assurance that contributions and loan payments are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 6—Plan Distributions and Payments

Controls provide reasonable assurance that plan distributions and payments to participants are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 7—Loan Requests

Controls provide reasonable assurance that loan requests are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 8—Fees

Controls provide reasonable assurance that requests for new fee setup, changes, corrections, terminations, and reversals are completely and accurately processed and recorded in the ABC

Recordkeeping application in a timely manner.

Control Objective 9—Investment Income

Controls provide reasonable assurance that investment income, dividends, corporate actions, and participant account values are completely and accurately calculated, processed, and recorded in a timely manner.

Control Objective 10—New Fund Setup and Changes

Controls provide reasonable assurance that new funds and changes to funds are authorized and completely and accurately implemented in a timely manner.

Control Objective 11—Asset Purchases and Redemption

Controls provide reasonable assurance that asset purchase and redemption transactions are authorized and completely and accurately traded and recorded in a timely manner.

Control Objective 12—Plan and Participant Statement Reporting

Controls provide reasonable assurance that plan and participant statements are accurate, complete, and provided to or sent to the plan sponsors or participants in a timely manner in accordance with contractual agreements.

Control Objective 13—Reconciliations

Controls provide reasonable assurance that cash and security positions are completely and accurately reconciled between the ABC Recordkeeping application and the depositories in a timely manner.

Control Objective 14—System Development and Change Management

Controls provide reasonable assurance that changes to the ABC Recordkeeping application, other programs, and related data management systems are authorized, tested, documented, approved, and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' financial reporting and to support user entities' internal control over financial reporting.

Control Objective 15—Logical Security

Controls provide reasonable assurance that logical access to programs, data, the ABC Recordkeeping application, and computer resources that may affect user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Control Objective 16—Computer Operations

Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and that deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner, with respect to user entities' internal control over financial reporting.

Control Objective 17—Network Infrastructure

Controls provide reasonable assurance that network infrastructure is configured as authorized,

with respect to user entities' internal control over financial reporting, to support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances and to protect data from unauthorized changes.

Control Objective 18—Data Transmissions

Controls provide reasonable assurance that data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely, with respect to user entities' internal control over financial reporting.

Control Objective 19—Physical Security

Controls provide reasonable assurance that physical access to computer and other resources, with respect to user entities' internal control over financial reporting, is restricted to authorized and appropriate personnel.

Control Objective 20—Data Backups

Controls provide reasonable assurance that data and systems are backed up regularly and available for restoration in the event of processing errors or unexpected processing interruptions, with respect to user entities' internal control over financial reporting.

Section 5: Other Information Presented by Management of Example Service Organization

- Business Continuity Planning
...
- Management's Response to Exceptions Identified
...

Appendix B

Illustrative Type 2 Reports—Inclusive Method, Including Illustrative Management Representation Letters

This appendix contains two illustrative type 2 reports. In example 1, the service organization uses one subservice organization and presents that subservice organization using the inclusive method. In example 2, the service organization uses two subservice organizations and presents one subservice organization using the inclusive method and the other subservice organization using the carve-out method.

The two illustrative type 2 reports in this appendix contain all of the required components¹¹ of a type 2 report; however, for brevity, the illustrative reports do not include all the elements that might be described in a type 2 report. Ellipses (...) or parenthetical notes to readers indicate places where detail has been omitted from the illustrative reports.

The control objectives and controls specified by the service organizations in examples 1 and 2, as well as the tests performed by the service auditor, are presented for illustrative purposes only. They are not intended to represent a complete or standard set of control objectives, controls, or tests of controls that would be appropriate for all service organizations. The determination of the appropriate control objectives, controls, and tests of controls for a specific service organization can be made only in the context of specific facts and circumstances. Accordingly, it is expected that actual type 2 reports will contain differing control objectives, controls, and tests of controls that are tailored to the service organization that is the subject of the engagement.

This appendix also contains illustrative representation letters for the service organization and subservice organization following each example.

The following chart identifies features of each illustrative type 2 report included in this appendix.

Summary of Features of Illustrative Type 2 Reports in Appendix B

Example Number and Name of Service Organization	Type of System Provided by the Service Organization	Name of Subservice Organization and Method of	Service Provided by the Subservice Organization(s)	Are Complementary User Entity Controls or	Format of the Type 2 Report
--	--	--	---	--	------------------------------------

¹¹ The required components of a type 1 report are the service auditor's report, management of the service organization's written assertion, and management's description of the service organization's system. The required components of a type 2 report are the service auditor's report, management of the service organization's written assertion, management's description of the service organization's system, and the service auditor's description of tests of controls and results thereof.

		Presentation		Complementary Subservice Organization Controls Required by the Service Organization?	
1. XYZ Service Organization	Defined contribution recordkeeping system	ABC Subservice Organization— Inclusive method	Maintenance and support of ABC Recordkeeping application	Service Organization requires complementary user entity controls	Narrative containing four report components referred to as sections 1, 2, 3, and 4
2. XYZ Service Organization	Defined contribution recordkeeping system	ABC Subservice Organization— Inclusive method and Computer Subservice Organization— Carve-out method	Maintenance and support of ABC Recordkeeping application Hosting services	Service Organization requires complementary user entity controls and complementary subservice organization controls	Narrative containing four report components referred to as sections 1, 2, 3, and 4

In example 1, XYZ Service Organization provides defined contribution recordkeeping services and uses the ABC Recordkeeping application. It outsources aspects of the maintenance and support of the ABC Recordkeeping application to ABC Subservice Organization and uses the inclusive method to present ABC Subservice organization.

The following is some information about the responsibilities of the service organization and subservice organization and the features of this type 2 report with respect to the use of the inclusive method for ABC Subservice Organization:

- ABC Subservice Organization prepares a description of its application maintenance and support services; that description is included in XYZ Service Organization’s description of its defined contribution recordkeeping system.
- The title of the description of the service organization’s system is “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System”; the title of the description does not mention ABC Subservice Organization.
- “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System” includes the control objectives and related controls of XYZ Service Organization and the relevant controls of ABC Subservice Organization.
- The service auditor’s report indicates that
— the service auditor examined XYZ Service Organization’s description of its

defined contribution recordkeeping system and ABC Subservice Organization's description of its application maintenance and support services, both of which are included in the "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "XYZ Service Organization's Assertion" and "ABC Subservice Organization's Assertion" (assertions).

- ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. XYZ Service Organization's description of its defined contribution recordkeeping system includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization.
- XYZ Service Organization's assertion states that
 - XYZ Service Organization uses ABC Subservice Organization for application maintenance and support services.
 - XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization.
- ABC Subservice Organization's assertion states that
 - ABC Subservice Organization provides application maintenance and support services to XYZ Service Organization and that those services are part of XYZ Service Organization's defined contribution recordkeeping system.
 - ABC Subservice Organization is responsible for the description of ABC Subservice Organization's application maintenance and support services provided to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system, which is included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" ...

Example 1: Service Organization Presents Subservice Organization Using the Inclusive Method, Complementary User Entity Controls Are Required, and Description Includes Other Information

XYZ Service Organization

Report on XYZ Service Organization's Description of its Defined Contribution

Recordkeeping System and on the Suitability of the Design and Operating Effectiveness of Its Controls

Changes to this type 2 report related to the use of the inclusive method and the need for complementary user entity controls are shown in boldface italics; deleted language is indicated by strikethrough. This type 2 report includes the following sections:

- Section 1: The independent service auditor's report
- Section 2: Management of XYZ Service Organization's assertion,
Management of ABC Subservice Organization's assertion¹²
- Section 3: Management of XYZ Service Organization's description of its system, which includes aspects of ABC Subservice Organization's services
- Section 4: The service auditor's description of tests of controls and results

Table of Contents

Section Number	Title of Section
1	Independent Service Auditor's Report
2	XYZ Service Organization's Assertion ABC Subservice Organization's Assertion
3	Description of XYZ Service Organization's Defined Contribution Recordkeeping System Overview of XYZ Service Organization Scope of the Description Internal Control Framework—XYZ Service Organization Control Environment Risk Assessment Process Monitoring Activities Information and Communications

¹² In example 1 of appendix B, there are two versions of management of ABC Subservice Organization's assertion. Version 1 of the assertion is predicated on the assumption that the service organization is responsible for evaluating whether the controls in the description, including the subservice organization's controls, are suitably designed and operating effectively to achieve the related control objectives. Version 2 of the assertion is predicated on the assumption that the subservice organization is responsible for evaluating the suitability of the design and operating effectiveness of its controls to achieve one or more related control objectives.

	Control Activities Internal Control Framework—ABC Subservice Organization Defined Contribution Plan Setup Control Objectives and Related Controls ¹³ <i>Complementary User Entity Controls</i>
4	Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Section 1: Independent Service Auditor’s Report

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization’s description of its defined contribution recordkeeping system *and ABC Subservice Organization’s description of its application maintenance and support services, both of which are included in* entitled “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System” for processing user entities’ transactions throughout the period January 1, 201X, to December 31, 201X, (description), and the suitability of the design and operating effectiveness of *XYZ Service Organization’s and ABC Subservice Organization’s* controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in “XYZ Service Organization’s Assertion” *and “ABC Subservice Organization’s Assertion”* (assertions). *ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. XYZ Service Organization’s description includes a description of ABC Subservice Organization’s application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including controls relevant to the control objectives stated in the description.*¹⁴ The controls and control objectives included in the description are those that management of XYZ Service Organization *and management of ABC Subservice Organization* believe are likely to be relevant to user entities’ internal control over financial reporting, and the description does not include those aspects of the defined contribution recordkeeping system that

¹³ In this illustrative report, the control objectives and related controls are included in section 4, “Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results.” This avoids the need to repeat the control objectives and related controls in two sections.

¹⁴ If the subservice organization’s control objectives were presented separately in the description, the wording of this sentence would read: “XYZ Service Organization’s description includes a description of ABC Subservice Organization’s application maintenance and support services used by XYZ Service Organization to process transactions for its user entities as well as relevant control objectives and related controls of ABC Subservice Organization.”

are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization and the subservice organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, XYZ Service Organization ***and ABC Subservice Organization*** ~~has~~ ***have*** ~~provided~~ ~~an~~***their*** assertions about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. XYZ Service Organization ***and ABC Subservice Organization*** ~~is~~ ***are*** responsible for preparing the description and ***their*** assertions, including the completeness, accuracy, and method of presentation of the description and assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertions, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertions, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 201X, to December 31, 201X. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertions.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated

in the description.

- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization **and subservice organization** in **their** ~~its~~ assertions.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on such user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization **or subservice organization** may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization **or subservice organization** may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in XYZ Service Organization's assertion **and ABC Subservice Organization's assertion**,

- a. the description fairly presents XYZ Service Organization's defined contribution recordkeeping system **and ABC Subservice Organization's application maintenance and support services** that ~~was~~ **were** designed and implemented throughout the period January 1, 201X, to December 31, 201X.
- b. the controls **of XYZ Service Organization and ABC Subservice Organization** related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 201X, to December 31, 201X, **and user entities applied the complementary user entity controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.**
- c. the controls **of XYZ Service Organization and ABC Subservice Organization** operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 201X, to December 31, 201X, **if complementary user entity controls assumed in the design of XYZ Service Organization's controls operated effectively throughout the period January 1, 201X, to**

December 31, 201X.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of XYZ Service Organization, user entities of XYZ Service Organization's defined contribution recordkeeping system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Section 2: XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's defined contribution recordkeeping system entitled "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

XYZ Service Organization uses ABC Subservice Organization, a subservice organization, to provide application maintenance and support services. XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including controls relevant to the control objectives stated in the description.¹⁵ ABC Subservice Organization's assertion is presented in section 2.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related

¹⁵ If the subservice organization's control objectives and related controls are presented separately in the description, the wording of this sentence would read: "XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including relevant control objectives and related controls of ABC Subservice Organization."

controls at the service organization. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the defined contribution recordkeeping system made available to user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions including, if applicable,
 - (1) the types of services provided including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the system captures and addresses significant events and conditions other than transactions.
 - (5) the process used to prepare reports and other information for user entities.
 - (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - (7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

- ii. includes relevant details of changes to the service organization's system during the period covered by the description.
 - iii. 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 user entities of the system and their user auditors, and may not, therefore, include every aspect of the defined contribution recordkeeping system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives ***if user entities applied the complementary user entity controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.*** The criteria we used in making this assertion were that
- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
 - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 2: ABC Subservice Organization's Assertion

Version 1: Illustrative Assertion by Management of Subservice Organization; Service Organization is Responsible for Evaluating All Controls in the Description

Version 1 of ABC Subservice Organization's assertion is predicated on the assumption that the service organization is responsible for evaluating whether the controls included in the description, including the subservice organization's controls, are suitably designed and operating effectively to achieve the related control objectives.

ABC Subservice Organization's Assertion

ABC Subservice Organization provides application maintenance and support services to XYZ Service Organization. The services provided by ABC Subservice Organization are part of XYZ Service Organization's defined contribution recordkeeping system. We are responsible for the description of ABC Subservice Organization's application maintenance and support services provided to XYZ Service Organization and user entities of XYZ Service Organization's defined

contribution record keeping system, which is included in “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System” for processing user entities’ transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities’ financial statements.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents ABC Subservice Organization’s application maintenance and support services made available to XYZ Service Organization and user entities of XYZ Service Organization’s defined contribution recordkeeping system during some or all of the period January 1, 20X1, to December 31, 201X, for processing their transactions, as it relates to controls that are likely to be relevant to user entities’ internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the application maintenance and support services made available to XYZ Service Organization and user entities of XYZ Service Organization’s defined contribution recordkeeping system were designed and implemented to process relevant user entity transactions, including, if applicable,
 - (1) the types of services provided by ABC Subservice Organization including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of ABC Subservice Organization’s procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the application maintenance and support services capture and address significant events and conditions other than transactions.
 - (5) the process used to prepare reports and other information for user entities.

- (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - (7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- ii. includes relevant details of changes to ABC Subservice Organization's services during the period covered by the description.
 - iii. does not omit or distort information relevant to ABC Subservice Organization's services, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the defined contribution recordkeeping system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. ABC Subservice Organization's controls related to the control objectives stated in the description were operating as described throughout the period January 1, 201X, to December 31, 201X. The criteria we used in making this assertion were that
 - i. the controls were consistently applied as described, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Version 2: Illustrative Assertion by Management of Subservice Organization; Subservice Organization is Responsible for Evaluating Subservice Organization's Controls Included in Description

Version 2 of ABC Subservice Organization's assertion is predicated on the assumption that the subservice organization is responsible for evaluating the design and operating effectiveness of its controls to achieve one or more related control objectives.

To illustrate the differences in this version of the assertion as compared to version 1 of the assertion, new language is shown in boldface italics and deleted language is shown by strikethrough.

ABC Subservice Organization's Assertion

ABC Subservice Organization provides application maintenance and support services to XYZ Service Organization. The services provided by ABC Subservice Organization are part of XYZ

Service Organization's defined contribution recordkeeping system. We are responsible for the description of ABC Subservice Organization's application maintenance and support services provided to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system, which is included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, when assessing the risks of material misstatement of user entities' financial statements.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents ABC Subservice Organization's application maintenance and support services made available to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system during some or all the period January 1, 20X1, to December 31, 201X, for processing their transactions, as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the application maintenance and support services made available to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system were designed and implemented to process relevant user entity transactions, including, if applicable,
 - (1) the types of services provided by ABC Subservice Organization, including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of ABC Subservice Organization's procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the application maintenance and support services capture and address significant events and conditions other than transactions.
 - (5) the process used to prepare reports and other information for user entities.

- (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - (7) ~~the~~ **XYZ Service Organization's** specified control objectives and **ABC Subservice Organization's** controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the subservice organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- ii. includes relevant details of changes to ABC Subservice Organization's services during the period covered by the description.
 - iii. does not omit or distort information relevant to ABC Subservice Organization's services, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the application maintenance and support services that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. ABC Subservice Organization's controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X. The criteria we used in making this assertion were that
 - i. *the risks that threaten the achievement of the control objectives stated in the description have been identified by management of ABC Subservice Organization.*
 - ii. *ABC Subservice Organization's controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent those control objectives stated in the description from being achieved.*
 - iii. ABC Subservice Organization's controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3: Description of XYZ Service Organization's Defined Contribution Recordkeeping System

Overview of XYZ Service Organization

XYZ Service Organization is located in Los Angeles, California, and provides defined contribution plan recordkeeping services to corporations, unions, and nonprofit customers (user entities) across the U.S. These services are provided using a proprietary ABC Recordkeeping

application developed and maintained by XYZ Service Organization.

Services provided as part of its defined contribution plan recordkeeping services include the following:

- Benefit plan setup and maintenance
-
-

XYZ Service Organization uses ABC Subservice Organization, a subservice organization, to provide application maintenance and support services for the ABC Recordkeeping application. The description includes the control objectives and related controls of XYZ Service Organization and the relevant controls of ABC Subservice Organization.

ABC Subservice Organization is located in Phoenix, Arizona, and provides application maintenance and support services for the ABC Recordkeeping application used by XYZ Service Organization. The ABC Recordkeeping application resides on servers in the XYZ Service Organization data center. ABC Subservice Organization provides application maintenance and support services for the ABC Recordkeeping application used by XYZ Service Organization including software enhancements or change requests originating from XYZ Service Organization.

Scope of the Description

This description of XYZ Service Organization's defined contribution recordkeeping system ***and ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization*** addresses only XYZ Service Organization's defined contribution recordkeeping system ***and ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization*** provided to user entities and excludes other services provided by XYZ Service Organization. The description is intended to provide information for user entities of the defined contribution recordkeeping system and their independent auditors, who audit and report on such user entities' financial statements (or internal control over financial reporting), to be used in obtaining an understanding of the defined contribution recordkeeping system and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of XYZ Service Organization's defined contribution recordkeeping system.

Internal Control Framework—XYZ Service Organization

This section provides information about the five interrelated components of internal control at XYZ Service Organization, including XYZ Service Organization's

- control environment,

- risk assessment process,
- monitoring activities,
- information and communications, and
- control activities.

[Note to readers: For brevity, the remainder of XYZ Service Organization’s description of the components of its internal control framework is not included here. Assume that the description of the components of XYZ Service Organization’s internal control framework would be the same as the description provided in example 1 of appendix A.]

Internal Control Framework—ABC Subservice Organization

This section provides information about the five interrelated components of internal control at ABC Subservice Organization, including ABC Subservice Organization’s

- control environment,
- risk assessment process,
- monitoring activities,
- information and communications, and
- control activities.

[Note to readers: For brevity, the remainder of ABC Subservice Organization’s description of the components of its internal control framework is not included here. Assume that the description of the components of ABC Subservice Organization’s internal control framework would follow the same approach used in example 1 of appendix A, with content that is tailored to the services provided by ABC Subservice Organization.]

Defined Contribution Plan Setup

Plan Setup

The new accounts team works with plan sponsors, prior recordkeeping service providers, and third-party administrators to facilitate the setup and conversion of the plan in the ABC Recordkeeping application. After receipt of a signed and authorized administrative services agreement from the plan sponsor, a member of the service organization’s new accounts team begins the process of preparing the file for upload into the ABC Recordkeeping application. The new accounts team member uses a new accounts setup checklist to ensure that the plan is completely and accurately set up in the ABC Recordkeeping application. Once the plan is ready

for upload, a new accounts team manager approves the file upload and signs the checklist as evidence of approval.

After the plan has been set up in the system, the new accounts team manager compares the date the plan is to be implemented in the system to the date in the administrative services agreement to ensure that the plan will be implemented timely. The new accounts team manager also reconciles the dollar total of the plan entered in the system to the dollar total provided by the plan's sponsor or prior recordkeeper. Any differences are investigated and resolved. The new accounts team manager completes the checklist to evidence that the reconciliation was performed and that the dollar totals were reconciled.

After the plan has been set up in the ABC Recordkeeping application, a second new accounts team manager reviews the plan information entered in the ABC Recordkeeping application and compares that information to the information in the supporting document provided by the plan sponsor or prior recordkeeper to ensure that the plan was completely and accurately set up in the system. The second new accounts team manager also completes the checklist to evidence that the dollar totals were reconciled and signs the checklist to evidence that the review was performed.

Plan Conversions

For plans set up on the ABC Recordkeeping application from prior recordkeepers, the new accounts team works with...

Plan Changes

For any changes to plans already set up on the ABC Recordkeeping application, the

[Note to readers: For brevity, the following aspects of XYZ Service Organization's description of its defined contribution recordkeeping system are not presented in this illustrative type 2 report.]

Plan administration

Participant administration

Transfers and changes in investment allocation

Contributions and loan payments

Plan distributions and payments

Loan requests

Fees

Investment income

New fund setup and changes

Asset purchases and redemption

Plan and participant statement reporting

Reconciliations

System development and change management

XYZ Service Organization uses the ABC Recordkeeping application to support its defined contribution recordkeeping services provided to user entities. The ABC Recordkeeping application was developed by ABC Subservice Organization, which is located in Phoenix, AZ. XYZ Service Organization uses a licensed version of the software from ABC Subservice Organization, which is responsible for providing ongoing maintenance and support of the application through the issuance of periodic software releases. Software releases are issued at least two times a year and patches or other less significant programming changes are issued on an as-needed basis. The ABC Recordkeeping application resides on servers located in the XYZ Service Organization's data center at its Los Angeles, CA, corporate headquarters. ABC Subservice Organization's application development activities follow a standard system development life cycle (SDLC), which is outlined in ABC Subservice Organization's change management policy.

ABC Recordkeeping application changes can be initiated to (1) enhance the ABC Recordkeeping software product, (2) correct software defects, and (3) address specific requests originating from licensed users of the software, for example, XYZ Service Organization. All ABC software enhancements or change requests must be formally documented on a change request form, entered into the IT ticketing system, approved by authorized ABC personnel, and forwarded to ABC Subservice Organization's product development group for approval. All change requests initiated by XYZ Service Organization must be approved by the XYZ Service Organization chief information officer and submitted to the ABC client service representative for processing by ABC personnel.

After review by the product development group, an evaluation is performed to determine whether the nature of the change requires the completion of a requirements analysis. Once the requirements analysis is completed and reviewed, the request is either approved or denied by the product development group. If approved, the approval is documented in the ticketing system and the request is forwarded to the programming development group for development and coding. Any requests originating from user entities are returned to the user entity for approval prior to proceeding with any development activities. All such requests affecting XYZ Service Organization must be approved by the XYZ Service Organization chief information officer.

The programming development group focuses on the development and coding of the request to meet its overall design and system requirements. All development activity is performed in the development environment. Once development or coding has been completed, the change is

tested in the development environment. Upon successful completion of testing, the quality assurance group is notified that the request is ready for quality assurance testing and review.

Upon notification by the development group, the quality assurance group moves the change into the quality assurance environment for testing. Testing is performed and documented by quality assurance staff and test results are reviewed and approved by quality assurance management. ABC Subservice Organization maintains separate environments for development, quality assurance testing, and production. Major system changes require user acceptance testing to determine whether the program change satisfies the user's requirements. XYZ Service Organization requires user acceptance testing for all major enhancements and changes to the ABC Recordkeeping software prior to production implementation of any such changes or releases into its production environment. All such testing is performed by the XYZ quality assurance group and must be approved by the XYZ chief information officer. The XYZ Service Organization maintains separate environments for testing and production.

If any defects or issues are found during the quality assurance testing process, they are tracked in the ABC ticketing system. Once testing is satisfactorily completed, the ABC quality assurance director approves the program change for production implementation and records the approval in the ticketing software.

The ABC technical services group is then notified that the change is ready for production implementation. Any changes ready for production implementation for XYZ Service Organization must be approved by the XYZ chief information officer before implementation into the XYZ production environment. Developers do not have access to the production environment to implement changes. ABC Subservice Organization uses the version control software tool to maintain version control over the ABC Recordkeeping program source code, and any changes to the production code are logged by the software. Access to the version control software is restricted to authorized personnel.

If an ABC Recordkeeping software problem or issue is reported by a user entity, the ABC customer service group is responsible for receiving and processing all such requests or incidents. When a call is received from the user entity, the client service representative logs the incident in the ticketing software, describes the problem, and issues a ticket. Issues are then escalated to the appropriate departments, and the problem or issue is prioritized, assigned to personnel for resolution, and documented in the ticketing application. If the problem requires a program change, the above process is followed for any IT programming requests. After the problem is resolved, the client service team notifies the customer and closes the ticket.

[Note to readers: For brevity, the following aspects of XYZ Service Organization's description of its defined contribution recordkeeping system are not presented in this illustrative type 2 report.]

Logical security

Network infrastructure

Computer operations

Data transmission

Physical security

Data backup

Control Objectives and Related Controls

XYZ Service Organization has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in section 4, “Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results,” and are an integral component of XYZ Service Organization’s description of its defined contribution recordkeeping system.

Complementary User Entity Controls

XYZ Service Organization’s controls related to the defined contribution recordkeeping system cover only a portion of overall internal control for each user entity of XYZ Service Organization. It is not feasible for the control objectives related to recordkeeping services to be achieved solely by XYZ Service Organization. Therefore, each user entity’s internal control over financial reporting should be evaluated in conjunction with XYZ Service Organization’s controls and the related tests and results described in section 4 of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable.¹⁶ In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control to determine whether the identified complementary user entity controls have been implemented and are operating effectively.

Section 4: Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

[Note to readers: For brevity, the details of “Information Provided by the Independent Service Auditor” are not presented in this illustrative report. An example of the detail in that section is

¹⁶ There is no prescribed format for presenting the complementary user entity controls. They may be listed in section 4 following the control objectives, tests of controls, and results of tests to which they apply, or they may be listed in the description of the service organization’s system in section 3. If listed in section 3, the complementary user entity controls should identify the control objectives to which they apply.

included in section 4 of example 1 in appendix A.]

[Note to readers: For brevity, XYZ Service Organization's description of its controls and the independent service auditor's description of tests of controls and results for control objectives 1–13 are not presented in this illustrative type 2 report.]

Control Objective 1—Defined Contribution Plan Setup

Controls provide reasonable assurance that defined contribution plans set up on the ABC Recordkeeping application are authorized by plan sponsors and completely and accurately processed and recorded in a timely manner.

Control Objective 2—Plan Administration

Controls provide reasonable assurance that changes to plan data are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 3—Participant Administration

Controls provide reasonable assurance that participant enrollments and changes to participant data are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 4—Transfers and Changes in Investment Allocations

Controls provide reasonable assurance that participant-initiated transfers and changes in investment allocations are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 5—Contributions and Loan Payments

Controls provide reasonable assurance that contributions and loan payments are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 6—Plan Distributions and Payments

Controls provide reasonable assurance that plan distributions and payments to participants are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 7—Loan Requests

Controls provide reasonable assurance that loan requests are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 8—Fees

Controls provide reasonable assurance that requests for new fee setup, changes, corrections, terminations, and reversals are completely and accurately processed and recorded in the ABC Recordkeeping application in a timely manner.

Control Objective 9—Investment Income

Controls provide reasonable assurance that investment income, dividends, corporate actions, and participant account values are completely and accurately calculated, processed, and recorded in a timely manner.

Control Objective 10—New Fund Setup and Changes

Controls provide reasonable assurance that new funds and changes to funds are authorized and completely and accurately implemented in a timely manner.

Control Objective 11—Asset Purchases and Redemption

Controls provide reasonable assurance that asset purchase and redemption transactions are authorized and completely and accurately traded and recorded in a timely manner.

Control Objective 12—Plan and Participant Statement Reporting

Controls provide reasonable assurance that plan and participant statements are accurate, complete, and provided to or sent to the plan sponsors or participants in a timely manner, in accordance with contractual agreements.

Control Objective 13—Reconciliations

Controls provide reasonable assurance that cash and security positions are completely and accurately reconciled between the ABC Recordkeeping application and the depositories in a timely manner.

Control Objective 14—Systems Development and Change Management

Controls provide reasonable assurance that changes to the ABC Recordkeeping application, other programs, and related data management systems are authorized, tested, documented, approved, and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' financial reporting and to support user entities' internal control over financial reporting.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
14.1 All ABC Recordkeeping software enhancements or change requests must be formally documented on a change request form and approved by authorized ABC Subservice Organization IT personnel. <i>(Control performed by ABC Subservice Organization)</i>	For a selection of ABC Recordkeeping changes implemented into production, inspected the change request form to determine whether the request was approved by the authorized ABC IT personnel.	No exceptions noted.
14.2 All ABC Recordkeeping software change requests originating from XYZ Service Organization must be approved by the XYZ Service Organization CIO.	For a selection of ABC Recordkeeping changes implemented into production and initiated by the XYZ Service Organization, inspected the change request form to determine whether the request was approved by the XYZ Service Organization CIO.	No exceptions noted.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
14.3 Once a requirements analysis is performed and documented (if required), the request is either approved or denied by the ABC product development group and documented in the ticketing system. <i>(Control performed by ABC Subservice Organization)</i>	For a selection of ABC Recordkeeping changes implemented into production, inspected the change request form to determine whether the request was approved or denied by the ABC product development group in the ticketing system.	No exceptions noted.
14.4 Any change requests approved for development (and impacting XYZ Service Organization) must be approved by XYZ CIO before development activities can commence.	For a selection of ABC Recordkeeping changes implemented into production, inspected related change documentation to determine whether the change was approved by the XYZ CIO before any development activities commenced.	No exceptions noted.
14.5 ABC Subservice Organization maintains separate environments for development, quality assurance and testing, and production. <i>(Control performed by ABC Subservice Organization)</i>	Inspected the ABC Subservice Organization URLs to determine whether separate environments exist for development, testing, and production.	No exceptions noted.
14.6 Testing of the software change is performed in the ABC quality assurance test environment by ABC QA personnel and, once testing is satisfactorily completed, the ABC QA director approves the change for production implementation and documents approval in the ticketing software. <i>(Control performed by ABC Subservice Organization)</i>	For a selection of ABC Recordkeeping changes implemented into production, inspected related change documentation to determine whether testing was performed by QA and whether the change was approved by the ABC QA director for production implementation.	No exceptions noted.
14.7 XYZ Service Organization requires user acceptance testing for all major enhancements and changes to the ABC Recordkeeping software prior to production implementation of any ABC Recordkeeping software changes or releases into its production environment. All such testing is performed by the XYZ QA group and must be approved by the XYZ CIO. XYZ Service Organization maintains separate environments for testing and production.	For a selection of ABC Recordkeeping changes implemented into production, inspected related change documentation to determine whether user acceptance testing was performed by XYZ QA personnel and approved by the XYZ CIO prior to implementation into the XYZ production environment. Inspected the XYZ Service Organization URLs to determine whether separate environments exist for testing and production.	No exceptions noted.

Controls Specified by XYZ Service Organization	Tests of Controls	Results of Tests
14.8 ABC Subservice Organization uses version control software to implement changes into production and to maintain version control over program source code. Any changes to the production code are logged by the software. <i>(Control performed by ABC Subservice Organization)</i>	Inspected the change control software and related logs to determine whether change control software is used to (1) implement changes into production and to maintain version control over program source code and (2) to log changes to production software.	No exceptions noted.
14.9 ...		
14.10 ...		
14.11 ...		

[Note to readers: For brevity, XYZ Service Organization's description of its controls and the independent service auditor's tests of controls and results for control objectives 15–20 are not presented in this illustrative type 2 report.]

Control Objective 15—Logical Security

Controls provide reasonable assurance that logical access to programs, data, the ABC Recordkeeping application, and computer resources that may affect user entities' internal control over financial reporting is restricted to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Control Objective 16—Computer Operations

Controls provide reasonable assurance that application and system processing are authorized and completely and accurately executed in a timely manner and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner, with respect to user entities' internal control over financial reporting.

Control Objective 17—Network Infrastructure

Controls provide reasonable assurance that network infrastructure is configured as authorized, with respect to user entities' internal control over financial reporting, to support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances and to protect data from unauthorized changes.

Control Objective 18—Data Transmissions

Controls provide reasonable assurance that data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely, with respect to user entities' internal control over financial reporting.

Control Objective 19—Physical Security

Controls provide reasonable assurance that physical access to computer and other resources, with respect to user entities' internal control over financial reporting, is restricted to authorized and appropriate personnel.

Control Objective 20—Data Backup

Controls provide reasonable assurance that data and systems are backed up regularly and available for restoration in the event of processing errors or unexpected processing interruptions, with respect to user entities' internal control over financial reporting.

**Illustrative Representation Letter from Management of the Service Organization for
Example 1: Management of the Service Organization Presents the Subservice Organization
Using the Inclusive Method**

[XYZ Service Organization's Letterhead]

*[Date]*¹⁷

[Service Auditor's Name]

[Address]

In connection with your engagement to report on XYZ Service Organization's description of its defined contribution recordkeeping system and ABC Subservice Organization's description of its application maintenance and support services, both of which are included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description)¹⁸ and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria in "XYZ Service Organization's Assertion" and "ABC Subservice Organization's Assertion" (assertions), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description fairly presents the system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X, and whether the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives, based on the criteria described in the assertions.

¹⁷ This representation letter should be dated as of the date of the service auditor's report.

¹⁸ The title of management's description of the service organization's system included in management's representation letter should be the same as the title included in management's description of the service organization's system, in management's assertion, and in the service auditor's report.

ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. The services provided by ABC Subservice Organization are part of our defined contribution recordkeeping system. The description includes a description of ABC Subservice Organization's services, including controls of ABC Subservice Organization relevant to the control objectives stated in the description. ABC Subservice Organization has provided a separate assertion attached to the description relevant to the services provided by ABC Subservice Organization.

We confirm, to the best of our knowledge and belief, as of *[date of this letter]*, the following representations made to you during your examination:¹⁹

1. We reaffirm our assertion attached to the description.
2. We have evaluated the fairness of the presentation of the description and the suitability of the design and operating effectiveness of our controls and ABC Subservice Organization's controls to achieve the related control objectives stated in the description, and all relevant matters have been considered and reflected in our evaluation and in our assertion.
3. We have disclosed to you any of the following of which we are aware:
 - a. Misstatements including omissions in the description
 - b. Instances in which our controls or ABC Subservice Organization's controls were not suitably designed and implemented
 - c. Instances in which our controls or ABC Subservice Organization's controls did not operate effectively or as described
 - d. Any communications from regulatory agencies, user entities, or others affecting the fairness of the presentation of the description or the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description, including communications received between the end of the period addressed in our assertion and the date of your report
 - e. All other known matters contradicting the fairness of the presentation of the description, the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description, or our assertion
4. We acknowledge responsibility for our assertion and for
 - a. the fairness of the presentation of the description and the suitability of the design and

¹⁹ If management does not provide one or more of the written representations requested by the service auditor, the service auditor should discuss the matter with management, evaluate the effect of such exclusions, and take appropriate action, which may include disclaiming the opinion or withdrawing from the engagement.

- operating effectiveness of the controls to achieve the related control objectives stated in the description.
- b.* selecting the criteria stated in our assertion and determining that the criteria are appropriate for our purposes.
 - 5. We have disclosed to you any known events subsequent to the period covered by the description up to the date of this letter that would have a material effect on the fairness of the presentation of the description, the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description, or our assertion.
 - 6. We have disclosed to you any changes in the controls that are likely to be relevant to user entities' internal control over financial reporting occurring through the date of this letter.
 - 7. We have provided you with all information and access that is relevant to your examination and to our assertion.
 - 8. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the fairness of the presentation of the description or the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description.
 - 9. We have responded fully to all inquiries made to us by you during the examination.
 - 10. We have disclosed to you any of the following of which we are aware:
 - a.* Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the fairness of the presentation of the description or the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description
 - b.* Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization that may affect one or more user entities
 - c.* Knowledge of any actual, suspected, or alleged fraud by our management or the service organization's employees that could adversely affect the fairness of the presentation of the description of the service organization's system or the completeness or achievement of the control objectives stated in the description

[Add any other representations about matters the service auditor deems appropriate or matters relevant to special circumstances, such as industry-specific matters.]

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion on the fairness of the presentation of the description and on the

suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on your examination, and that your procedures were limited to those that you considered necessary for that purpose.

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]

**Illustrative Representation Letter from Management of the Subservice Organization for
Example 1: Management of the Service Organization Presents the Subservice Organization
Using the Inclusive Method**

[ABC Subservice Organization's Letterhead]

*[Date]*²⁰

[Service Auditor's Name]

[Address]

In connection with your engagement to report on XYZ Service Organization's description of its defined contribution recordkeeping system and ABC Subservice Organization's description of its application maintenance and support services, both of which are included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description)²¹ and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "XYZ Service Organization's Assertion" and "ABC Subservice Organization's Assertion" (assertions), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description fairly presents XYZ Service Organization's defined contribution recordkeeping system and ABC Subservice Organization's application maintenance and support services that were designed and implemented throughout the period January 1, 201X, to December 31, 201X, and whether the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives, based on the criteria identified in the assertions.

The description includes certain services provided by ABC Subservice Organization to or on behalf of XYZ Service Organization. We are responsible for the portion of the description that

²⁰ This representation letter should be dated as of the date of the service auditor's report.

²¹ The title of management's description of the service organization's system included in management's representation letter should be the same as the title included in management's description of the service organization's system, in management's assertion, and in the service auditor's report.

describes ABC Subservice Organization's services and activities.

We confirm, to the best of our knowledge and belief, as of *[date of this letter]*, the following representations made to you during your examination:²²

1. We reaffirm our assertion attached to the description.
2. We have evaluated the fairness of the presentation of our portion of the description and the suitability of the design and operating effectiveness of our controls as described,²³ and all relevant matters have been considered and reflected in our evaluation and in our assertion.
3. We have disclosed to you any of the following of which we are aware:
 - a. Misstatements including omissions in the description
 - b. Instances in which controls were not suitably designed and implemented
 - c. Instances in which controls did not operate effectively or as described
 - d. Any communications from regulatory agencies, user entities, or others affecting the fairness of the presentation of our portion of the description or the suitability of the design or operating effectiveness of our controls as described, including communications received between the end of the period addressed in our assertion and the date of your report
 - e. All other known matters contradicting the fairness of the presentation of our portion of the description, the suitability of the design or operating effectiveness of our controls as described, or our assertion
4. We acknowledge responsibility for our assertion and for
 - a. the fairness of the presentation of our portion of the description and the suitability of the design and operating effectiveness of our controls as described.
 - b. selecting the criteria stated in our assertion and determining that the criteria are

²² If management does not provide one or more of the written representations requested by the service auditor, the service auditor should discuss the matter with management, evaluate the effect of such exclusions, and take appropriate action, which may include disclaiming the opinion or withdrawing from the engagement.

²³ The representations in this letter are predicated on the assumption that the service organization is responsible for evaluating whether the controls, including the subservice organization's controls, are suitably designed and operating effectively to achieve the related control objectives. The wording of the representations should be modified to reflect the relevant responsibilities, for example, if the subservice organization were responsible for evaluating the design and operating effectiveness of its controls to achieve one or more related control objectives.

appropriate for our purposes.

5. We have disclosed to you any known events subsequent to the period covered by the description up to the date of this letter that would have a material effect on the fairness of the presentation of the description, the suitability of the design or operating effectiveness of our controls as described, or our assertion.
6. We have disclosed to you any changes in our controls that are likely to be relevant to user entities' internal control over financial reporting occurring through the date of this letter.
7. We have provided you with all information and access that is relevant to your examination and to our assertion.
8. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the fairness of the presentation of our portion of the description or the suitability of the design or operating effectiveness of our controls as described.
9. We have responded fully to all inquiries made to us by you during the examination.
10. We have disclosed to you any of the following of which we are aware:
 - a. Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the fairness of the presentation of the description or the suitability of the design or operating effectiveness of our controls as described
 - b. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the subservice organization that may affect one or more user entities
 - c. Knowledge of any actual, suspected, or alleged fraud by our management or the subservice organization's employees that could adversely affect the fairness of the presentation of our portion of the description

[Add any other representations about matters the service auditor deems appropriate or matters relevant to special circumstances, such as industry-specific matters.]

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on your examination, and that your procedures were limited to those that you considered necessary for that purpose.

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]

Example 2: Service Organization Presents One Subservice Organization Using the Inclusive Method and Another Subservice Organization Using the Carve-out Method; Complementary User Entity and Complementary Subservice Organization Controls Are Required

In example 2, XYZ Service Organization outsources aspects of the maintenance and support of the ABC Recordkeeping application to ABC Subservice Organization and elects to use the inclusive method of presentation for ABC Subservice Organization. XYZ Service Organization also uses Computer Subservice Organization to provide hosting services and elects to use the carve-out method of presentation for the Computer Subservice Organization. In addition, complementary user entity and complementary subservice organization controls are required to achieve certain control objectives.

The following is some information about the responsibilities of XYZ Service Organization and ABC Subservice Organization and the features of this type 2 report with respect to the use of the inclusive method for ABC Subservice Organization:

- ABC Subservice Organization prepares a description of its application maintenance and support services; that description is included in XYZ Service Organization’s description of its defined contribution recordkeeping system.
- The title of the description of the service organization’s system is “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System”; the title does not mention ABC Subservice Organization.
- “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System” includes the control objectives and related controls of XYZ Service Organization and the relevant controls of ABC Subservice Organization.
- The service auditor’s report indicates that
 - the service auditor examined XYZ Service Organization’s description of its defined contribution recordkeeping system and ABC Subservice Organization’s description of its application maintenance and support services, both of which are included in “Description of XYZ Service Organization’s Defined Contribution Recordkeeping System” for processing user entities’ transactions throughout the period January 1, 201X, to December 31, 201X, (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in “XYZ Service Organization’s Assertion” and “ABC

Subservice Organization's Assertion" (assertions).

- ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. XYZ Service Organization's description of its defined contribution recordkeeping system includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization.
- XYZ Service Organization's assertion states that
 - XYZ Service Organization uses ABC Subservice Organization for application maintenance and support services.
 - XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization.
- ABC Subservice Organization's assertion states that
 - ABC Subservice Organization provides application maintenance and support services to XYZ Service Organization and that those services form a part of XYZ Service Organization's defined contribution recordkeeping system.
 - ABC Subservice Organization is responsible for the description of ABC Subservice Organization's application maintenance and support services provided to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system, which is included in the "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" ...

Changes to this type 2 report related to the use of the inclusive method and the need for complementary user entity and complementary subservice organization controls are shown in boldface italics; deleted language is indicated by strikethrough. This type 2 report includes the following sections:

- Section 1: The independent service auditor's report
- Section 2: Management of XYZ Service Organization's assertion
Management of ABC Subservice Organization's assertion
- Section 3: Management of XYZ Service Organization's description of its system and aspects of ABC Subservice Organization's services
- Section 4: The service auditor's description of tests of controls and results

**Report on XYZ Service Organization’s Description of its Defined Contribution
Recordkeeping System and on the Suitability of the Design and Operating
Effectiveness of Its Controls**

Table of Contents

Section Number	Title of Section
1	Independent Service Auditor’s Report
2	XYZ Service Organization’s Assertion ABC Subservice Organization’s Assertion
3	Description of XYZ Service Organization’s Defined Contribution Recordkeeping System <div style="padding-left: 40px;"> Overview of XYZ Service Organization Scope of the Description Internal Control Framework—XYZ Service Organization Control Environment Risk Assessment Process Monitoring Activities Information and Communications Control Activities Internal Control Framework—ABC Subservice Organization Defined Contribution Plan Setup Control Objectives and Related Controls²⁴ <i>Complementary Subservice Organization Controls</i> <i>Complementary User Entity Controls</i> </div>
4	Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Section 1: Independent Service Auditor’s Report

²⁴ In this illustrative report, the control objectives and related controls are included in section 4, “Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results.” This avoids the need to repeat the control objectives and related controls in two sections.

To: XYZ Service Organization

Scope

We have examined XYZ Service Organization's description of its defined contribution recordkeeping system and ***ABC Subservice Organization's description of its application maintenance and support services, both of which are included in*** entitled "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) and the suitability of the design and operating effectiveness of ***XYZ Service Organization's and ABC Subservice Organization's*** controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "XYZ Service Organization's Assertion" and "***ABC Subservice Organization's Assertion***" (assertions). ***ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization to process transactions for its user entities, including controls relevant to control objectives stated in the description.*** The controls and control objectives included in the description are those that management of XYZ Service Organization ***and management of ABC Subservice Organization*** believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the defined contribution recordkeeping system that are not likely to be relevant to user entities' internal control over financial reporting.

XYZ Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of XYZ Service Organization and ABC Subservice Organization and excludes the control objectives and related controls of the Computer Subservice Organization. The description also indicates that certain control objectives specified by XYZ Service Organization can be achieved only if complementary subservice organization controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with the related controls at XYZ Service Organization. Our examination did not extend to controls of the Computer Subservice Organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary Computer Subservice Organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In section 2, XYZ Service Organization ***and ABC Subservice Organization*** ~~has~~ ***have*** provided ~~an~~ ***their*** assertions about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control

objectives stated in the description. XYZ Service Organization **and ABC Subservice Organization** ~~is~~**are** responsible for preparing the description and **their** assertions, including the completeness, accuracy, and method of presentation of the description and assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertions, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertions, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 201X, to December 31, 201X. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertions.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization **and subservice organization** in **their** ~~its~~ assertions.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a **service organization or a**

subservice organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization ***or a subservice organization*** may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

Opinion

In our opinion, in all material respects, based on the criteria described in XYZ Service Organization's assertion ***and ABC Subservice Organization's assertion***

- a. the description fairly presents XYZ Service Organization's defined contribution recordkeeping system ***and ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization*** that ~~was~~*were* designed and implemented throughout the period January 1, 201X, to December 31, 201X.
- b. the controls ***of XYZ Service Organization and ABC Subservice Organization*** related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 201X, to December 31, 201X, ***and subservice organizations and user entities applied the complementary controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.***
- c. the controls ***of XYZ Service Organization and ABC Subservice Organization*** operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period January 1, 201X, to December 31, 201X, ***if complementary subservice organization and user entity controls assumed in the design of XYZ Service Organization's controls operated effectively throughout the period January 1, 201X, to December 31, 201X.***

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of XYZ Service Organization, user entities of XYZ Service Organization's defined contribution recordkeeping system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

[Service auditor's signature]

[Service auditor's city and state]

[Date of the service auditor's report]

Section 2: XYZ Service Organization's Assertion

We have prepared the description of XYZ Service Organization's defined contribution recordkeeping system entitled "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

XYZ Service Organization uses ABC Subservice Organization, a subservice organization, to provide application maintenance and support services. XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including controls relevant to the control objectives stated in the description.²⁵ ABC Subservice Organization's assertion is presented in section 2.

XYZ Service Organization also uses Computer Subservice Organization, a subservice organization, to provide hosting services. The description includes only the control objectives and related controls of XYZ Service Organization and ABC Subservice Organization and excludes the control objectives and related controls of the hosting subservice organization. The description also indicates that certain control objectives specified by XYZ Service Organization in the description can be achieved only if complementary subservice organization controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with the related controls at XYZ Service Organization. The description does not extend to controls of the Computer Subservice Organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of XYZ Service Organization's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

²⁵ If the control objectives and related controls for the subservice organization are presented separately in the description, the service auditor may consider changing the wording of this sentence to read: "XYZ Service Organization's description includes a description of ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization to process transactions for user entities, including relevant control objectives and related controls of ABC Subservice Organization."

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents the defined contribution recordkeeping system made available to user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions including, if applicable,
 - (1) the types of services provided, including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the system captures and addresses significant events and conditions other than transactions.
 - (5) the process used to prepare reports and other information for user entities.
 - (6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.
 - (7) the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
 - ii. includes relevant details of changes to the service organization's system during the period covered by the description.

- iii. 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 user entities of the system and their user auditors, and may not, therefore, include every aspect of the defined contribution recordkeeping system that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives ***if subservice organizations and user entities applied the complementary controls assumed in the design of XYZ Service Organization's controls throughout the period January 1, 201X, to December 31, 201X.*** The criteria we used in making this assertion were that
 - i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.
 - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 2: ABC Subservice Organization's Assertion

This assertion is predicated on the assumption that the service organization is responsible for evaluating whether the controls included in the description, including the subservice organization's controls, are suitably designed and operating effectively to achieve the related control objectives.

ABC Subservice Organization provides application maintenance and support services to XYZ Service Organization. The services provided by ABC Subservice Organization are part of XYZ Service Organization's defined contribution recordkeeping system. We are responsible for the description of ABC Subservice Organization's application maintenance and support services provided to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system, which is included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description) for user entities of the system during some or all of the period January 1, 201X, to December 31, 201X, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, when assessing the risks of material misstatement of user entities' financial statements.

We confirm, to the best of our knowledge and belief, that

- a. the description fairly presents ABC Subservice Organization's application maintenance and support services made available to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system during some or all of the period January 1, 20X1, to December 31, 201X, for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description
 - i. presents how the application maintenance and support services made available to XYZ Service Organization and user entities of XYZ Service Organization's defined contribution recordkeeping system were designed and implemented to process relevant user entity transactions including, if applicable,
 - (1) the types of services provided by ABC Subservice Organization, including, as appropriate, the classes of transactions processed.
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - (3) the information used in the performance of ABC Subservice Organization's procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.
 - (4) how the application maintenance and support services capture and address significant events and conditions other than transactions.
 - (5) the process used to prepare reports and other information for user entities.
 - (6) services performed by a subservice organization, if any, and whether the carve-out method or the inclusive method has been used in relation to them.
 - (7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - (8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities,

and monitoring activities that are relevant to the services provided.

- ii. includes relevant details of changes to ABC Subservice Organization's services during the period covered by the description.
 - iii. does not omit or distort information relevant to ABC Subservice Organization's services, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the application maintenance and support services that each individual user entity of the system and its auditor may consider important in its own particular environment.
- b. ABC Subservice Organization's controls related to the control objectives stated in the description were operating as described throughout the period January 1, 201X, to December 31, 201X. The criteria we used in making this assertion were that
- i. ABC Subservice Organization's controls were consistently applied as described, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section 3: Description of XYZ Service Organization's Defined Contribution Recordkeeping System

Overview of XYZ Service Organization

XYZ Service Organization is located in Los Angeles, California, and provides defined contribution plan recordkeeping services to corporations, unions, and nonprofit customers (user entities) across the U.S. These services are provided using a proprietary ABC Recordkeeping application system that was developed and is maintained by XYZ Service Organization.

Services provided as part of its defined contribution plan recordkeeping services include the following:

- Benefit plan setup and maintenance
-
-

XYZ Service Organization uses ABC Subservice Organization, a subservice organization, to provide application maintenance and support services. XYZ Service Organization also uses Computer Subservice Organization, a subservice organization, to provide hosting services.

ABC Subservice Organization

ABC Subservice Organization is located in Phoenix, Arizona, and provides application maintenance and support services for the ABC Recordkeeping application used by XYZ

Service Organization. The ABC Recordkeeping application resides on servers in the Computer Subservice Organization's data center. ABC Subservice Organization provides the following services to XYZ Service Organization:

- ***Application maintenance and support services for the ABC Recordkeeping application used by XYZ Service Organization including software enhancements or change requests originating from XYZ Service Organization***

Computer Subservice Organization

ABC Subservice Organization is located in Los Angeles, California, and provides computer hosting services for XYZ Service Organization. The ABC Recordkeeping application resides on servers hosted by Computer Subservice Organization at its data center in Los Angeles, California.

The description includes the control objectives and related controls of XYZ Service Organization and the relevant controls of ABC Subservice Organization and excludes the control objectives and related controls of the Computer Subservice Organization.

Scope of the Description

In accordance with the criteria in management's assertion, this description includes a description of XYZ Service Organization's defined contribution recordkeeping system provided to its user entities ***and ABC Subservice Organization's application maintenance and support services used by XYZ Service Organization and excludes the control objectives and related controls of the Computer Subservice Organization.*** The description is intended to provide information for user entities and their independent auditors to obtain an understanding of the system and controls in place over XYZ Service Organization's defined contribution recordkeeping system that are likely to be relevant to a user entity's internal control over financial reporting. The description of the system includes certain business process controls and information technology general controls that support the delivery of XYZ Service Organization's defined contribution recordkeeping system.

Internal Control Framework—XYZ Service Organization

This section provides information about the five interrelated components of control at XYZ Service Organization, including

- control environment,
- risk assessment,
- monitoring activities.
- information and communications, and

- control activities.

[Note to readers: For brevity, and except as noted below for monitoring activities, the remainder of XYZ Service Organization's description of the components of its internal control framework are not included here. Assume that the description of the components of XYZ Service Organization's internal control framework would be the same as the description provided in example 1 of appendix A.]

XYZ Service Organization employs a combination of ongoing and periodic monitoring activities to monitor that controls are functioning effectively and that risks are appropriately mitigated.

Ongoing Monitoring

The service organization uses a variety of reports and monitoring mechanisms to help ensure that controls are functioning as intended; these include

- electronic display of pending transactions and their status,
- deficiency and incident reporting,
- suspense account reporting,
- daily pricing variances,
- financial reconciliations,
- quality review results and reporting, and
- system processing monitoring and reporting.

Management regularly reviews and assesses business operations to determine that reporting and monitoring mechanisms are used and effective in managing the operations of the business, controls, and related risks.

Periodic Assessments and Monitoring

In addition to the ongoing monitoring activities described above, each business unit conducts specific evaluations of risks and controls to maximize the effectiveness of its operations.

The internal audit department performs internal audits of operations and controls to assess the effectiveness of controls. The results of audits and any identified deficiencies are reported to management as well as the audit committee. Management prepares and implements corrective measures to address any significant deficiencies.

Monitoring of the Subservice Organization

XYZ Service Organization uses Computer Subservice Organization, a subservice organization, to provide hosting services.

Management and Internal Audit of XYZ Service Organization receive and review the type 2 SOC 1[®] report of Computer Subservice Organization on annual basis. In addition, through its daily operational activities, management of XYZ Service Organization monitors the services performed by the Computer Subservice Organization to ensure operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes planned at the hosting facility, and to communicate any issues or concerns to Computer Subservice Organization management.

Internal Control Framework—ABC Subservice Organization

This section provides information about the five interrelated components of control at ABC Subservice Organization, including

- control environment,
- risk assessment,
- monitoring activities,
- information and communications, and
- control activities.

[Note to readers: For brevity, the remainder of ABC Subservice Organization’s description of the components of its internal control framework is not included here. Assume that the description of the components of ABC Subservice Organization’s internal control framework would follow the same approach used in example 1 of appendix A, with content that is tailored to the services provided by ABC Subservice Organization.]

[Note to readers: For brevity, the description of XYZ Service Organization’s defined contribution recordkeeping system is not presented here and would be the same as the description provided in example 1 of appendix B.]

Control Objectives and Related Controls

XYZ Service Organization has specified the control objectives and identified the controls that are designed to achieve the stated control objectives. The specified control objectives, related controls, and complementary user entity controls are presented in section 4, “Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results,” and are an integral component of XYZ Service Organization’s description of its defined contribution recordkeeping system.

Complementary Subservice Organization Controls (CSOC)

XYZ Service Organization’s controls relating to the defined contribution recordkeeping system cover only a portion of the overall internal control structure of each user entity of XYZ Service Organization. It is not feasible for the control objectives relating to recordkeeping services to be solely achieved by XYZ Service Organization. Therefore, each user entity’s internal control over financial reporting must be evaluated in conjunction with XYZ Service Organization’s controls and related testing detailed in section 4 of this report, taking into account the complementary subservice organization controls expected to be implemented at the subservice organization as described below.

	<i>Complementary Subservice Organization Control (CSOCs)</i>	<i>Related Control Objectives (CO)</i>
	<i><u>Computer Subservice Organization</u></i>	
1.	<i>The Computer Subservice Organization is responsible for maintaining logical security over the servers and other hardware devices upon which the ABC Recordkeeping application is hosted.</i>	<i>CO 16</i>
2.	<i>The Computer Subservice Organization is responsible for notifying XYZ Service Organization of any security incidents relating to security over the servers and other hardware devices upon which the ABC Recordkeeping application is hosted.</i>	<i>CO 16</i>
3.	<i>The Computer Subservice Organization is responsible for maintaining physical security over its data center in which the servers used to host the ABC Recordkeeping application are housed.</i>	<i>CO 20</i>
4.	

Complementary User Entity Controls

XYZ Service Organization’s controls relating to the defined contribution recordkeeping system cover only a portion of the overall internal control structure of each user entity of XYZ Service Organization. It is not feasible for the control objectives relating to recordkeeping services to be solely achieved by XYZ Service Organization. Therefore, each user entity’s internal control over financial reporting must be evaluated in conjunction with XYZ Service Organization’s controls and related testing detailed in section 4 of this report, taking into account the related complementary user entity controls identified under each control objective, where applicable.²⁶ In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control structure to determine if the identified complementary user entity controls are in place.

²⁶ There is no prescribed format for presenting complementary user entity controls. They may be listed in section 4 following the control objectives, tests of controls, and results of tests to which they apply, or they may be listed in the description of the service organization’s system in section 3. If listed in section 3, the complementary user entity controls should identify the control objectives to which they apply.

Section 4: Description of XYZ Service Organization’s Control Objectives and Related Controls, and Independent Service Auditor’s Description of Tests of Controls and Results

Information Provided by the Independent Service Auditor

[Note to readers: For brevity, the details of “Information Provided by the Independent Service Auditor” are not presented in this illustrative report. An example of the detail in that section is included in section 4 of example 1 in appendix A.]

[Note to readers: For brevity, the XYZ Service Organization’s description of its controls and the independent service auditor’s description of tests of controls and results for control objectives 1–20 are not presented in this illustrative type 2 report.]

Control Objective 1—Defined Contribution Plan Setup

Controls provide reasonable assurance that defined contribution plans set up on the ABC Recordkeeping application are authorized by plan sponsors and completely and accurately processed and recorded on a timely basis.

Control Objective 2—Plan Administration

Controls provide reasonable assurance that changes to plan data are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 3—Participant Administration

Controls provide reasonable assurance that participant enrollments and changes to participant data are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 4—Transfers and Changes in Investment Allocations

Controls provide reasonable assurance that participant-initiated transfers and changes in investment allocations are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 5—Contributions and Loan Payments

Controls provide reasonable assurance that contributions and loan payments are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 6—Plan Distributions and Payments

Controls provide reasonable assurance that plan distributions and payments to participants are authorized and completely and accurately processed and recorded in a timely manner.

Control Objective 7—Loan Requests

Controls provide reasonable assurance that loan requests are authorized and completely and

accurately processed and recorded in a timely manner.

Control Objective 8—Fees

Controls provide reasonable assurance that requests for new fee setup, changes, corrections, terminations, and reversals are completely and accurately processed and recorded in the ABC Recordkeeping application in a timely manner.

Control Objective 9—Investment Income

Controls provide reasonable assurance that investment income, dividends, corporate actions, and participant account values are completely and accurately calculated, processed and recorded in a timely manner.

Control Objective 10—New Fund Setup and Changes

Controls provide reasonable assurance that new funds and changes to funds are authorized and completely and accurately implemented in a timely manner.

Control Objective 11—Asset Purchases and Redemption

Controls provide reasonable assurance that asset purchase and redemption transactions are authorized and completely and accurately traded and recorded in a timely manner.

Control Objective 12—Plan and Participant Statement Reporting

Controls provide reasonable assurance that plan and participant statements are complete, accurate, and provided to or sent to the plan sponsors or participants in a timely manner, in accordance with contractual agreements.

Control Objective 13—Reconciliations

Controls provide reasonable assurance that cash and security positions are completely and accurately reconciled between the ABC Recordkeeping application and the depositories in a timely manner.

Control Objective 14—Systems Development and Change Management

Controls provide reasonable assurance that changes to the ABC Recordkeeping application, programs, and related data management systems are authorized, tested, documented, approved, and implemented to result in complete, accurate, and timely processing and reporting of transactions and balances relevant to user entities' financial reporting and to support user entities' internal control over financial reporting.

Control Objective 15—Logical Security

Controls provide reasonable assurance that logical access to programs, data, the ABC Recordkeeping application, and computer resources is restricted, with respect to user entities' internal control over financial reporting, to authorized and appropriate users and such users are restricted to performing authorized and appropriate actions.

Control Objective 16—Computer Operations

Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner and deviations, problems, and errors are

identified, tracked, recorded, and resolved in a complete, accurate, and timely manner, with respect to user entities' internal control over financial reporting.

Control Objective 17—Network Infrastructure

Controls provide reasonable assurance that network infrastructure is configured as authorized, with respect to user entities' internal control over financial reporting, to support the effective functioning of application controls to result in valid, complete, accurate, and timely processing and reporting of transactions and balances and to protect data from unauthorized changes.

Control Objective 18—Data Transmissions

Controls provide reasonable assurance that data transmissions between the service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely, with respect to user entities' internal control over financial reporting.

Control Objective 19—Physical Security

Controls provide reasonable assurance that physical access to computer and other resources, with respect to user entities' internal control over financial reporting, is restricted to authorized and appropriate personnel.

Control Objective 20—Data Backup

Controls provide reasonable assurance that data and systems are backed up regularly and available for restoration in the event of processing errors or unexpected processing interruptions, with respect to user entities' internal control over financial reporting.

**Illustrative Representation Letter From Management of the Service Organization for
Example 2: Management of the Service Organization Presents the Subservice Organization
Using the Inclusive Method**

[XYZ Service Organization's Letterhead]

*[Date]*²⁷

[Service Auditor's Name]

[Address]

In connection with your engagement to report on XYZ Service Organization's description of its defined contribution recordkeeping system and ABC Subservice Organization's description of its application maintenance and support services, both of which are included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities'

²⁷ This representation letter should be dated as of the date of the service auditor's report.

transactions throughout the period January 1, 201X, to December 31, 201X, (description)²⁸ and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria in “XYZ Service Organization’s Assertion” and “ABC Subservice Organization’s Assertion” (assertions), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description fairly presents the system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X, and whether the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives, based on the criteria described in the assertions.

ABC Subservice Organization is a subservice organization that provides application maintenance and support services to XYZ Service Organization. The services provided by ABC Subservice Organization are part of our defined contribution recordkeeping system. The description includes a description of ABC Subservice Organization’s services, including controls of ABC Subservice Organization relevant to the control objectives stated in the description. ABC Subservice Organization has provided a separate assertion attached to the description relevant to the services provided by ABC Subservice Organization.

We confirm, to the best of our knowledge and belief, as of *[date of this letter]*, the following representations made to you during your examination:²⁹

1. We reaffirm our assertion attached to the description.
2. We have evaluated the fairness of the presentation of the description and the suitability of the design and operating effectiveness of our controls and ABC Subservice Organization’s controls to achieve the related control objectives stated in the description, and all relevant matters have been considered and reflected in our evaluation and in our assertion.
3. We have disclosed to you any of the following of which we are aware:
 - a. Misstatements including omissions in the description
 - b. Instances in which our controls or ABC Subservice Organization’s controls were not suitably designed and implemented
 - c. Instances in which our controls or ABC Subservice Organization’s controls did not

²⁸ The title of management’s description of the service organization’s system included in management’s representation letter should be the same as the title included in management’s description of the service organization’s system, in management’s assertion, and in the service auditor’s report.

²⁹ If management does not provide one or more of the written representations requested by the service auditor, the service auditor should discuss the matter with management, evaluate the effect of such exclusions, and take appropriate action, which may include disclaiming the opinion or withdrawing from the engagement.

operate effectively or as described

- d. Any communications from regulatory agencies, user entities, or others affecting the fairness of the presentation of the description or the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description, including communications received between the end of the period addressed in our assertion and the date of your report
 - e. All other known matters contradicting the fairness of the presentation of the description, the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description, or our assertion
4. We acknowledge responsibility for our assertion and for
 - a. the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description.
 - b. selecting the criteria stated in our assertion and determining that the criteria are appropriate for our purposes.
5. We have disclosed to you any known events subsequent to the period covered by the description up to the date of this letter that would have a material effect on the fairness of the presentation of the description, the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description, or our assertion.
6. We have disclosed to you any changes in the controls that are likely to be relevant to user entities' internal control over financial reporting occurring through the date of this letter.
7. We have provided you with all information and access that is relevant to your examination and to our assertion.
8. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the fairness of the presentation of the description or the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description.
9. We have responded fully to all inquiries made to us by you during the examination.
10. We have disclosed to you any of the following of which we are aware:
 - a. Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the fairness of the presentation of the description or the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description

- b. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the service organization that may affect one or more user entities
- c. Knowledge of any actual, suspected, or alleged fraud by our management or the service organization's employees that could adversely affect the fairness of the presentation of the description of the service organization's system or the completeness or achievement of the control objectives stated in the description

[Add any other representations about matters the service auditor deems appropriate or matters relevant to special circumstances, such as industry-specific matters.]

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on your examination, and that your procedures were limited to those that you considered necessary for that purpose.

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]

Illustrative Representation Letter from Management of the Subservice Organization for Example 2: Management of the Service Organization Presents the Subservice Organization Using the Inclusive Method

[ABC Subservice Organization's Letterhead]

*[Date]*³⁰

[Service Auditor's Name]

[Address]

In connection with your engagement to report on XYZ Service Organization's description of its defined recordkeeping system and ABC Subservice Organization's description of its application maintenance and support services, both of which are included in "Description of XYZ Service Organization's Defined Contribution Recordkeeping System" for processing user entities' transactions throughout the period January 1, 201X, to December 31, 201X, (description)³¹ and

³⁰ This representation letter should be dated as of the date of the service auditor's report.

³¹ The title of management's description of the service organization's system included in management's representation letter should be the same as the title included in management's description of the service organization's system, in management's assertion, and in the service auditor's report.

the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in “XYZ Service Organization’s Assertion” and “ABC Subservice Organization’s Assertion” (assertions), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description fairly presents the system that was designed and implemented throughout the period January 1, 201X, to December 31, 201X, and whether the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period January 1, 201X, to December 31, 201X, to achieve those control objectives, based on the criteria identified in the assertions.

The description includes certain services provided by ABC Subservice Organization to or on behalf of XYZ Service Organization. We are responsible for the portion of the description that describes ABC Subservice Organization’s services and activities.

We confirm, to the best of our knowledge and belief, as of *[date of this letter]*, the following representations made to you during your examination:³²

1. We reaffirm our assertion attached to the description.
2. We have evaluated the fairness of the presentation of our portion of the description and the suitability of the design and operating effectiveness of our controls as described,³³ and all relevant matters have been considered and reflected in our evaluation and in our assertion.
3. We have disclosed to you any of the following of which we are aware:
 - a. Misstatements including omissions in the description
 - b. Instances in which controls were not suitably designed and implemented
 - c. Instances in which controls did not operate effectively or as described
 - d. Any communications from regulatory agencies, user entities, or others affecting the fairness of the presentation of our portion of the description or the suitability of the design or operating effectiveness of our controls as described, including

³² If management does not provide one or more of the written representations requested by the service auditor, the service auditor should discuss the matter with management, evaluate the effect of such exclusions, and take appropriate action, which may include disclaiming the opinion or withdrawing from the engagement.

³³ The representations in this letter are predicated on the assumption that the service organization is responsible for evaluating whether the controls, including the subservice organization’s controls, are suitably designed and operating effectively to achieve the related control objectives. The wording of the representations should be modified to reflect the relevant responsibilities, for example, if the subservice organization were responsible for evaluating the design and operating effectiveness of its controls to achieve one or more related control objectives.

communications received between the end of the period addressed in our assertion and the date of your report

- e. All other known matters contradicting the fairness of the presentation of our portion of the description, the suitability of the design or operating effectiveness of our controls as described, or our assertion
4. We acknowledge responsibility for our assertion and for
 - a. the fairness of the presentation of our portion of the description and the suitability of the design and operating effectiveness of our controls as described.
 - b. selecting the criteria stated in our assertion and determining that the criteria are appropriate for our purposes.
5. We have disclosed to you any known events subsequent to the period covered by the description up to the date of this letter that would have a material effect on the fairness of the presentation of the description, the suitability of the design or operating effectiveness of our controls as described, or our assertion
6. We have disclosed to you any changes in our controls that are likely to be relevant to user entities' internal control over financial reporting occurring through the date of this letter.
7. We have provided you with all information and access that is relevant to your examination and to our assertion.
8. We believe the effects of uncorrected misstatements, if any, are immaterial, individually and in the aggregate, to the fairness of the presentation of our portion of the description or the suitability of the design or operating effectiveness of our controls as described.
9. We have responded fully to all inquiries made to us by you during the examination.
10. We have disclosed to you any of the following of which we are aware:
 - a. Actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the fairness of the presentation of the description or the suitability of the design or operating effectiveness of our controls as described
 - b. Instances of noncompliance with laws and regulations or uncorrected misstatements attributable to the subservice organization that may affect one or more user entities
 - c. Knowledge of any actual, suspected, or alleged fraud by our management or the subservice organization's employees that could adversely affect the fairness of the presentation of our portion of the description

[Add any other representations about matters the service auditor deems appropriate or matters

relevant to special circumstances, such as industry-specific matters.]

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on your examination, and that your procedures were limited to those that you considered necessary for that purpose.

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]

[Name and title of appropriate member of management]
