SOC 2℠

User Guide

for Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

AICPA®

ISACA®
Trust in, and value from, information systems

Disclaimer
ISACA® has designed this publication, *SOC 2SM User Guide* (the "Work"), primarily as an educational resource for user entities. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, user entities should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Feedback: *www.isaca.org/SOC2*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

AICPA
1211 Avenue of the Americas
New York, NY 10036-8775
Phone: +1.212.596.6200
Fax: +1.212.596.6213
Email: *service@aicpa.org*
Web site: *www.aicpa.org*

Follow AICPA on Twitter Feeds, LinkedIn Networks, Facebook Communities and YouTube Channels: *www.aicpa.org/News/Pages/SocialMedia.aspx#twitter*

SOC 2SM User Guide
ISBN 978-1-60420-260-1
Printed in the United States of America

Acknowledgments

ISACA wishes to recognize:

Development Team
Floris Ampe, CISA, CGEIT, CRISC, CIA, ISO 27001, PwC, Belgium
Bart Peeters, CISA, PwC, Belgium
Sara Weiland, CISA, PwC LLP, USA

Work Group
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
George Galindo, CISA, CPA, PwC, USA
Chris Halterman, CPA, Ernst & Young LLP, USA
Mary Stoltenberg-Smith, CISA, CISM, CRISC, Federal Reserve Bank Chicago, USA

Expert Reviewers
Barbara Baldwin, SVP, Ocean First Bank, USA
Rich Chew, CISA, CISM, CGEIT, Emerald Management Group, USA
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA
Chris Kradjan, CRISC, CPA, Moss Adams LLP, USA
John W. Lainhart IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, USA
Jon Long, CISA, CompliancePoint, USA
Rena Mears, CISA, CISSP, CPA, Deloitte & Touche, USA
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM Global Business Services, USA
Richard Reinders, GCFA, GCIH, Sec+, Lake Trust Credit Union, USA
Lily Shue, CISA, CISM, CGEIT, CRISC, Sunera LLC, USA
David A. Williams, CRISC, PMP, Ocean First Bank, USA
Daniel Zimerman, CISA, CEH, CISSP, CPT, GCIH, IQ Solutions, USA

ISACA Board of Directors
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, International President
Allan Boardman, CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, Morgan Stanley, UK, Vice President
Juan Luis Carselle, CISA, CGEIT, CRISC, Wal-Mart, Mexico, Vice President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, 6 Sigma, Quest Software, Spain, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management Inc., USA, Vice President
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., (retired), USA, Past International President
John Ho Chi, CISA, CISM, CRISC,CBCP, CFE, Ernst & Young LLP, Singapore, Director
Krysten McCabe, CISA, The Home Depot, USA, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, BRM Holdich, Australia, Director

Acknowledgments (cont.)

Knowledge Board
Marc Vael, Ph.D., CISA, CISM, CGEIT, CRISC, CISSP, Valuendo, Belgium, Chairman
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Thomas E. Borton, CISA, CISM, CRISC, CISSP, Cost Plus, USA
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Salomon Rico, CISA, CISM, CGEIT, Deloitte, Mexico
Steven E. Sizemore, CISA, CIA, CGAP, Texas Health and Human Services Commission, USA

Guidance and Practices Committee
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
Dan Haley, CISA, CGEIT, CRISC, MCP, Johnson & Johnson, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Pelissari, Brazil
Jotham Nyamari, CISA, Deloitte, USA
Connie Lynn Spinelli, CISA, CRISC, CFE, CGMA, CIA, CISSP, CMA, CPA, GRC Solutions LLC, USA
John William Walker, CISM, CRISC, FBCS CITP, ITPC Secure Bastion Ltd., UK
Siang Jun Julia Yeo, CISA, CPA (Australia), Visa Worldwide Pte. Limited, Singapore
Nikolaos Zacharopoulos, CISA, CISSP, DeutschePost–DHL, Germany

Special Recognition
ISACA New Jersey Chapter for its financial support

ISACA and IT Governance Institute® (ITGI®) Affiliates and Sponsors
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Socitum Performance Management Group
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

ASIS International
Hewlett-Packard
IBM
Symantec Corp.

Table of Contents

Page intentionally left blank

Section 1. Introduction

Background

The ever-growing emphasis on governance, risk management and compliance has caused enterprises to focus on internal controls over all aspects of their operations. As part of this focus, many enterprises that outsource functions or processes (user entity) to a service organization are requiring the service organization to provide evidence of effectiveness of design and operation of its controls to ensure that the organization's control requirements have been met. This has increased the need for service organizations to provide assurance, trust and transparency over their controls.

Since 1992, the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No. 70 (SAS 70) report has been the primary way that service organizations provided evidence of the effectiveness of the design and operation of their controls that affected customer financial reporting. Over time, however, SAS 70 reports became more than just financial reporting and effective 15 June 2011 this report was superseded by three Service Organization Control (SOC) reports—SOC 1, SOC 2 and SOC 3. The SOC 1 report is prepared in accordance with Statements on Standards for Attestation Engagements (SSAE 16) for reporting on controls relevant to internal control over financial reporting (ICFR), an attestation engagement commonly known as a Service Organization Controls 1 report. The SOC 2 and SOC 3 reports are prepared in accordance with SSAE's AT Section 101 and used to report on controls relevant to security, availability, processing integrity, confidentiality or privacy.

From the early days of the SAS 70 report, user entities have sought a "SAS 70-like" report that addresses more than just their financial reporting controls. In May 2011, AICPA issued *Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* (SOC 2), which uses AICPA's Trust Services Principles and Criteria to report on controls at a service organization. The SOC 2 report provides service organizations and user entities more flexibility related to both compliance and operational reporting controls. Although the distribution is restricted, the limitations make it as broad as possible and available to customers who can understand the report's content. However, the report should not be distributed to unintended users such as other user entity vendors unless an agreement has been made with the service organization.

The SOC 2 report is designed to meet user entity requirements beyond that of a SSAE 16 SOC 1 report. A SOC 2 report addresses risk of IT-enabled systems and privacy programs beyond the controls necessary for financial reporting. Additionally, SOC 2 uses predefined standard control criteria for each of the defined principles (see section 3), which allows for more direct comparison of service organizations' internal control environments.

Scope and Approach

This user guide focuses on the SOC 2 report issued by service organizations relevant to the effectiveness of the design and operation of their controls related to security, availability, processing integrity, confidentiality or privacy. The guide is structured as follows:

- Section 2 briefly describes various service organization reports (SOC 1, SOC 2 and SOC 3).
- Section 3 provides a detailed explanation of the standards used and the types, scope and content for a SOC 2 report.
- Section 4 evaluates how to determine the user entity's needs when obtaining a SOC 2 report.
- Section 5 explains how to communicate the user entity's needs to the service organization.
- Section 6 explains how to interpret the SOC 2 report provided by the service organization.

Purpose of the *SOC 2 User Guide* (Benefits and Value)

AICPA is the world's largest association representing the accounting profession, with nearly 377,000 members in 128 countries. It sets attestation and ethical standards for the profession and US auditing standards for audits of private companies; nonprofit organizations; and federal, state and local governments. AICPA is responsible for establishing the professional standard, guidance and criteria used for SOC 1 and SOC 2 reports. It also provides standards that external user auditors apply when using a SOC 1 report as part of a financial audit.

With 100,000 constituents in 180 countries, ISACA is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. It develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. ISACA supports user entities in understanding the AICPA guidance and develops materials to help them evaluate and implement it.

Together, AICPA and ISACA are releasing this guide to provide the reader with information needed to interpret the SOC 2 reports received from a service organization. This guide also complements the companion piece for the SOC 1 guide which can be found at *www.isaca.org/service-auditor-standard.*

Who Should Use This Guide?

When a user entity engages a service organization to perform key processes or functions on its behalf, the user entity transfers some of its risk and certain activities related to its risk mitigation responsibility to the service organization. This transfer exposes the user entity to additional risk related to the service organization and its systems. Although the user entity's management can delegate tasks or functions to a service organization, the responsibility for the performance of those tasks cannot be delegated, it remains with the user entity. The user entity's management remains fully accountable for managing the user entity's own risk and the service organization's risk for the services being performed.

To assess and address the risk associated with an outsourced service, the user entity's management needs information about the effectiveness of the design and operation of a service organization's controls over the system through which the services are delivered. To gather this information, user entity management may ask the service organization for a SOC 2 report. The report may address the design and operating effectiveness of controls over the service organization's systems that are relevant to the systems' security, availability or processing integrity, or it may cover the confidentiality or privacy of the information processed for user entities.

Management at the user entity is held accountable by those charged with governance (e.g., the board of directors), customers, shareholders, regulators and other affected parties for establishing effective internal control over outsourced functions. This guide is intended for those evaluating a service organization's SOC 2 report as part of a governance, risk and compliance (GRC) program; vendor assessment; security evaluation; business continuity plan (BCP) or other control evaluation. It may also be useful to those considering requesting a SOC 2 report from an existing vendor that does not currently provide a report or a new vendor as part of the due diligence or request for proposal (RFP) process. Specific users of this guide might include:

- Management of the user entity
- Those in procurement and contract negotiation
- Those overseeing vendor management
- Practitioners evaluating or reporting on controls at a user entity
- Independent auditors of user entities
- Regulators
- Those performing services related to controls at the service organization, such as a service auditor reporting on controls at a user entity that is also a service provider to other user entities

Page intentionally left blank

Section 2. The Foundation— Types of SOC Reports

What Are SOC Reports?

There are three types of SOC reports that can be issued by the service organization, depending on the intended purpose:

- SOC 1—*Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting* (ICFR)
- SOC 2—*Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* in accordance with AT Section 101 and Trust Services Principles Criteria and Illustrations TPA Section 100
- SOC 3—*Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy* in accordance with AT Section 101 and Trust Services Principles Criteria and Illustrations TPA Section 100

SOC 1 and SOC 2 reports are intended to provide user entities with a description of the service organization's system as well as a detailed understanding of the design of controls at that service organization and the tests performed by the service auditor to support his/her conclusions on the operating effectiveness of those controls. Meaning that the service auditor evaluates that controls have been put in place by the service organization to address the identified risk and whether those controls are performed (operating) over the period of time specified; e.g., 1 January 2012 to 31 December 2012. This gives the user entity the understanding when evaluating the SOC report where comfort over controls for the services outsourced can be achieved.

SOC 1 addresses service organization system controls that are likely to be relevant to user entities' financial statements; SOC 2 addresses the system controls that are relevant to one or more of the Trust Services principles of *Security, Availability, Processing Integrity, Confidentiality* or *Privacy*, regardless of whether the controls are significant to user entities' internal controls over financial reporting. Both SOC 1 and SOC 2 reports are intended for an exclusive distribution list and are restricted-use reports (e.g., service and user organization management, internal/external auditors). However, the SOC 2 report can be distributed to any customer who can understand the report's content with the service organization's agreement. The report should not be distributed to unintended users, such as subvendors, without the service organization's permission.

A SOC 3 report covers the same principles as a SOC 2 report, but does not include the detailed understanding of the design of controls and the tests performed by the service auditor. This report provides the auditor's opinion on whether the service organization maintains effective controls over its systems and is typically intended for users who do not require a more thorough report that includes a detailed description of the design of controls or tests performed by the service auditor.

SOC 3 reports are intended for general use and can be freely distributed and publicly promoted via use of the AICPA SOC 3 seal on the service organization's web site.

Similarities and Differences Between the SOC Reports

The SOC 1 and SOC 2 reports are meant to complement each other and have several similarities and differences. **Figure 1** compares the two reports to emphasize their purpose, focus, distribution and use.

Figure 1—Comparison of SOC 1 and SOC 2 Reports

	SOC 1 Report	SOC 2 Report
Professional standard under which the engagement is performed	SSAE No. 16, *Reporting on Controls at a Service Organization* (AICPA, Professional Standards, AT Section 801)	AT Section 101, Attest Engagements (AICPA, Professional Standards)
Other applicable AICPA guidance	AICPA, *Service Organizations: Applying SSAE No, 16, Reporting on Controls at a Service Organization Guide (SOC 1)*	• AICPA, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2)—AICPA Guide* • TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy*
Subject matter of the engagement	Service organization system controls likely to be relevant to user entities' internal control over financial reporting	• Service organization system controls relevant to security, availability, processing integrity, confidentiality or privacy • If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices
Purpose of the report	• Provide the user entity's auditor with information and a certified public accountant's (CPA's) opinion over controls at a service organization that may directly impact the user entity's financial statements. • Support the user entity's auditor understanding of the design and implementation of controls at the service organization while assessing the user entity's internal control environment.	• Provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about suitability of the design of controls at the service organization relevant to **security, availability, processing integrity, confidentiality or privacy** • A SOC 2 Type 2 report provides evidence that controls at the service organization are operating effectively

Figure 1—Comparison of SOC 1 and SOC 2 Reports *(cont.)*

	SOC 1 Report	SOC 2 Report
Purpose of the report *(cont.)*	• If a SOC 1 Type 2 report, can be used as audit evidence that controls at the service organization are operating effectively	• A SOC 2 Type 2 report that addresses privacy also provides information and a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices
Where each report is applicable and why	• User entity's financial audit • User entity's evaluation of internal control over financial reporting • User entity's evaluation of its internal control in accordance with the US Sarbanes-Oxley Act • Mapped to financial assertions and support of the financial audit	• GRC/vendor management programs • Vendor due diligence • Regulatory compliance • Mapped to compliance and operational contols
Components of the report	• Description of the service organization's system • Written assertion by management • Opinion on the fairness of the presentation of the description of the service organization's system; the suitability of the design of the controls to achieve specified control objectives; and, in a Type 2 report, the operating effectiveness of those controls • In a Type 2 report, a description of the service auditor's tests of the controls and the results of the tests	Same as SOC 1 report.
Period covered by the report	• Type 1 gives an opinion for a specific point of time. • Type 2 covers a period of time defined in the system description.	Same as SOC 1 report.

Figure 1—Comparison of SOC 1 and SOC 2 Reports *(cont.)*

	SOC 1 Report	SOC 2 Report
Examples of areas in which some entities/industries might consider each type of report	• Maintenance accounting software • Trust departments of banks and insurance companies • Custodians for investment companies • Mortgage servicers or depository institutions that service loans for others • Other financial transactions or financially significant systems	• Hosting and support services (e.g., cloud computing, IT infrastructure, data center management, logical security management) • Sales force automation • Health care claims management and processing • Printing of customer statements where processing integrity and confidentiality are important • Trust departments of banks and insurance companies • Custodians for investment companies, storage and vaulting firms • Mortgage servicers or depository institutions that service loans for others • Other nonfinancial transaction processing or systems that are not financially significant
Benefits	• Independent examination of controls • Concept of Type 1 (design of controls only) and Type 2 (design and operating effectiveness of controls) • Focus on internal controls over financial reporting • Control objectives defined by management of the service organization • Includes details of the processing and controls at a service organization, the tests performed by the service auditor, and results of the tests	• May be better suited for outsourced technology-focused services and assessment of overall technology controls • Independent examination of controls • Concept of Type 1 (design of controls only) and Type 2 (design and operating effectiveness of controls) • Reporting on nonfinancial controls • Adherence to the defined principles and related criteria, making reports comparable from different service organizations; omissions stated in the auditor’s opinion • Used to emphasize system security, availability, processing integrity, confidentiality and privacy • Includes details of the processing and controls at a service organization, the tests performed by the service auditor, and results of the tests • May address privacy and availability, generally excluded from a SOC 1 report (especially privacy) • Distribution of report not as restricted as a SOC 1 report; includes individuals with the ability to understand the content of the report

Intended Application/Use of Each Report

SOC 1

The following examples of SOC 1 reports clarify the intended use:

- A user entity outsources the maintenance of its accounting software to a service organization. The management of the user entity would like to know that the service organization performs its operations in a way that does not result in misstatement in its financial reporting. Therefore, management requests a SOC 1 report to ensure that the risk related to the financial reporting process is adequately addressed by the service organization's effectively designed and operated controls.
- Investor entities may purchase mortgage loans or participation interests in such loans from thrifts, banks or mortgage companies. These loans become assets of the investor entities, and the sellers may continue to service the loans. Because the investor entities may have little or no contact with the mortgage servicers other than receiving monthly payments and reports from the mortgage servicer, the investor entities may request a SOC 1 report to ensure that risk related to the financial reporting process are adequately addressed by the seller's service organization.

SOC 2

The SOC 2 report can be used for a range of services provided by the service organization to the user entity, to provide the user entity comfort over the controls at the service organization relevant to security, availability, processing integrity, confidentiality or privacy. The following are examples of potential SOC 2 reports and their intended use:

- With regard to printing service for client trust and/or tax statements, the service organization is responsible for transferring the required information to the correct printer and printing the documents. This requires that the service organization provide the user entity with comfort over the confidentiality, security and privacy of the information being printed, which may be accomplished by issuance of a SOC 2 report.
- Application service providers (ASPs) provide packaged software applications and a technology environment that enables customers to process operational transactions. An ASP may specialize in providing a particular software package solution to its users, may provide services similar to traditional mainframe data center service bureaus, may perform business processes for user entities that they traditionally had performed themselves, or may provide some combination of these services. This requires that the service organization provide the user entity with comfort over the confidentiality, security and privacy of the information being printed, which may be accomplished by issuance of a SOC 2 report.

A SOC 2 report cannot be extended to include financial controls, but can include principles and criteria that are related to IT general controls.

- For example, a cloud provider is hosting a financial application. The user entity may require the system details from the cloud provider and may also need to gain comfort over the internal controls on financial reporting for the financial system. In this case, testing performed to prepare a SOC 2 report can be used to prepare a SOC 1 report to provide assurance over the IT general controls of the financial application. **Figure 2** summarizes the main reasons to use a SOC 2 report vs. SOC 1.

Figure 2—Reasons to Use a SOC 2 Report vs. a SOC 1 Report

- No financial-related transaction processing for clients
- Distribution to management of user entities and other specified parties, not just to auditors of the user entity
- A need to obtain assurance over security, availability, processing integrity, confidentiality and privacy
- Establishment of common and consistent control criteria
- A need to demonstrate compliance with regulatory, contractual or other requirements

Section 3. Using the SOC 2 Report

A user entity that relies on a service organization to process, maintain or store the user entity's information needs to understand and monitor the systems being used for the services to:

- Assess stewardship or accountability
- Assess its ability to comply with contractual responsibilities, commitments to stakeholders, and certain aspects of laws and regulations—e.g., the US Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA)
- Assess the integrity of the information provided

To assess the relevance of a SOC 2 report, the user entity must understand the report coverage and whether:

- The services relevant to the user entity are included.
- There is a clear system description providing sufficient detail to understand the processes at the service organization.
- The controls are relevant, demonstrate consideration of planned reliance on the operational and compliance controls, and take into account the relationship to complementary user entity activities.
- The report covers a period of time or a point in time, and that time period is relevant to the user entity's coverage needs.
- There is contiguous coverage between reports, and relevant locations are included that the user entity considers in scope.
- User entity auditors and others in the user organization planning to rely on the SOC 2 report may be require to examine the design and effectiveness of user complementary controls.

The Standard Used for a SOC 2 Report

It is important to understand the delineated boundaries of the system under examination for the Trust Services principles and criteria of security, availability, processing integrity, confidentiality and privacy. Knowing these boundaries helps the user entity understand the control coverage over the processing relevant to their environment.

Following is a brief overview of AICPA's AT Section 101 and the Trust Services principles used by service organizations to create SOC 2 reports for distribution to user entities.

AT Section 101, Attest Engagements (AICPA, Professional Standards)

The standard used for a SOC 2 report is AICPA's AT Section 101, Attest Engagements, which applies to engagements in which a practitioner is engaged to issue an examination of an assertion about subject matter that is the responsibility of another party.

Trust Services Principles and Criteria

Trust Services are defined as a set of professional attestation and advisory services based on principles and criteria that address the risk and opportunities of IT-enabled systems and privacy programs. Trust Services principles and criteria are issued by AICPA and the Canadian Institute of Chartered Accountants (CICA). *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* provides guidance when providing assurance services or advisory services (or both) on IT-enabled systems including electronic commerce (e-commerce) systems. It is particularly relevant when providing services related to security, availability, processing integrity, confidentiality and privacy.

The Trust Services principles and criteria are organized into four broad areas:

- **Policies**—The entity has defined and documented its policies relevant to the particular principle. (The term "policies" as used here refers to written statements that communicate management's intent, objectives, requirements, responsibilities and standards for a particular subject.)
- **Communication**—The entity has communicated its defined policies to responsible parties and authorized users of the system.
- **Procedures**—The entity has placed procedures in operation to achieve its principles in accordance with its defined policies.
- **Monitoring**—The entity monitors the system and takes action to maintain compliance with its defined policies.

The Trust Services introduce a list of criteria against which these four areas are evaluated to assess whether one or more of the following five principles, which were developed by AICPA and CICA for use by practitioners in the performance of trust services engagements, have been achieved:

- **Security**—The system is protected against unauthorized access (both physical and logical).
- **Availability**—The system is available for operation and use as committed or agreed.
- **Processing integrity**—System processing is complete, accurate, timely and authorized.
- **Confidentiality**—Information designated as confidential is protected as committed or agreed.
- **Privacy**—Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in *Generally Accepted Privacy Principles* (GAPP) issued by AICPA and CICA.

Types of SOC 2 Reports

There are two types of SOC 2 reports that can be received by the user entity from the service organization. When evaluating the type of report provided it is important to note that a service auditor report may not include both a Type 1 opinion for certain applicable Trust Service criteria and controls and a Type 2 opinion for other applicable Trust Service criteria and controls. The service auditor is engaged to perform either a Type 1 or Type 2 engagement.[1] The following describes both types of reports:

- Type 1 reports on the design of controls and only at a specific point in time.
- Type 2 reports on the design and operating effectiveness of controls covering a period of time.

Type 1

For a Type 1 report, the service auditor provides an opinion as to whether:

- The service organization's description "fairly presents" the system that was designed and implemented.
- The controls were suitably designed to meet the criteria as of a specified date.

Type 1 reports do not address the operating effectiveness of controls, nor do they provide an opinion over a period of time. This means that the report only provides information on controls that are in place (designed) at a specific point in time and not whether the controls are operating on a continuous basis throughout a specified time period. Due to the limited scope of the service auditor's opinion in a Type 1 report, a Type 2 report is generally preferable unless the user entity wants only to understand the nature of the controls at the service organization and whether they are adequately designed.

Type 2

For a Type 2 report, the service auditor provides an opinion on whether:

- The service organization's description "fairly presents" the system that was designed and implemented.
- The controls were suitably designed to meet the criteria.
- The controls operated effectively during the specified period of time.
- The service organization is in compliance with the commitments in its statement of privacy practices, if the report covers the privacy principle.

A Type 2 report is necessary if the user entity plans to use the report for reliance on internal control or if the user entity's management or auditor plans to use the report for the assessment of internal controls.

The Type 2 report opinion clearly identifies the period of interest. If the period of time is for less than two months, the user entity will likely need to consider whether the resulting report is useful, particularly if many of the controls are performed on a monthly or quarterly basis.

If the controls have changed, or if the service provider discloses deviations, the user entity should evaluate the impact of those changes and/or deviations and may choose to perform additional test procedures to gain comfort over the controls in place at the service organization. Additionally, it is important for the user entity to receive the report as soon as possible upon publication so the information is most relevant to the organization.

[1] AICPA, *SOC 2 Audit Guide*, USA, 2012, Section 1.31

Content of a SOC 2 Report

Several components comprise a SOC 2 report and they vary depending on whether it is a Type 1 or Type 2 report. In most cases, SOC 2 reports do not include all the principles—only those that the service organization's management deemed appropriate for the report. Therefore, it is important for the user entity to evaluate the report and determine which principles are covered.

SOC 2 Report Section 1 (Type 1 and Type 2 Reports)

Management's description of the service organization's system

This section should clearly describe the systems, services, transactions, reports and business processes performed at the service organization that are relevant to the specified TSP principles and criteria that are the subject of the report. This will enable the user entity to gain an understanding of the structure and processes supported for the specific services being provided. In addition, the depth of detail should enable the user entity to clearly identify risk areas where the principles and the control criteria should be put in place by the service organization. In this way, the user entity can identify any design gaps within the report.

The description of the system made by the management of the service organization generally includes the following information:

- Types of services provided by the service organization and the related procedures by which they are provided
- Types of transactions processed and procedures by which they are performed
- System components including infrastructure, software, people, procedures, data
- System boundaries or aspects relevant to the report
- How reports are prepared for user entities
- How incorrect information is identified and corrected, and how information is transferred to user entity reports
- How the system captures and addresses significant events and conditions, including notification to users
- Principles, control criteria and complementary user entity controls
- The risk assessment process, information and communication systems, and monitoring controls
- The scope of the report (specific principles covered)
- Servicing locations included in the scope of the report and any differences among the processes that are performed at the various locations
- The description of various oversight and monitoring functions in place that relate to the services provided
- The description of the various laws and regulations with which the organization complies, and how the organization monitors compliance
- The identification of any services performed by a subservice provider and the vendor management controls in place

Example of Management's Description of Information Security Logical Access Provisioning

New user accounts are provisioned by the access management group within the security team, or by persons or systems delegated to do so on their behalf. New internal user access requests must be submitted via the Ticketing System to the access management group and must come from an authorized requestor—either the new user's manager or human resources (HR) department. Requests for access changes or user termination are submitted through the Ticketing System by the user's manager. New users are created using access management utilities or they can be created via a scripted process if there are multiple users to be created.

A terminated user's group access membership is revoked and the user's account is disabled automatically via a script based on termination data fed from the personnel management system. User accounts are reviewed monthly by the access management group and any account that has not been used within the last 90 days is disabled.

On a quarterly basis, user managers receive a system-generated report of the system access of their personnel. Managers are required to request changes as needed and confirm that all remaining access is appropriate. The security manager monitors receipt of confirmations from the managers and follows up on any confirmations not received.

SOC 2 Report Section 2 (Type 1 and Type 2 reports)

A written assertion by management of the service organization

Management's assertions communicate the following to the user entity, and increase the service organization's ownership and strengthen the trust relationship between the two entities:

- The description of the system fairly presents the system in place.
- Controls stated in management's description are suitably designed and operated effectively throughout the specified period to meet applicable control criteria.
- The specific Trust Services principles and criteria that were the subject of management's assertion
- Compliance with the commitments in the statement of privacy practices throughout the specified period (This applies when the system description addresses the privacy principle.)
- The process used to prepare and deliver reports and other information to user entities and other parties
- For information provided to, or received from, subservice organizations and other parties:
  - How the information is provided or received and the role of the subservice organizations and other parties
  - The procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls

- For each principle being reported on, the related criteria in TSP Section 100 (applicable Trust Services criteria) and the related controls designed to meet those criteria, including, as applicable, the following:
  - Complementary user entity controls contemplated in the design of the service organization's system
  - Controls at the subservice organization when the inclusive method is used to present a subservice organization
- If the service organization presents the subservice organization using the carve-out method:
  - The nature of the services provided by the subservice organization
  - Each of the applicable Trust Services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria
- Any applicable Trust Services criteria that are not addressed by a control and the reasons why
- Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable Trust Services criteria

It is important to note that a SOC 2 report may not include all of the principles. The service organization, with input from its users, identifies the principles that the report will cover.

Example of a Written Assertion by Management of the Service Organization

We have prepared the attached description titled "Description of [CLIENT]'s Company-Controlled Data Center System for the Period 1 April 2011, to 30 September 2011" (Description) based on the criteria in the following items (a)(i)–(ii), which are the criteria for a description of a service organization's system in paragraphs 1.33–.34 of *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2)—AICPA Guide* (Description Criteria). The Description is intended to provide users with information about the Company-Controlled Data Center System, particularly system controls intended to meet the criteria for the availability principle set forth in TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids) (applicable Trust Services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the Company-Controlled Data Center System throughout the period 1 April 2011 to 30 September 2011, based on the following Description Criteria:
   i. The Description contains the following information:
      1. The types of services provided

Example of a Written Assertion by Management of the Service Organization *(cont.)*

2. The components of the system used to provide the services, which are the following:
   - **Infrastructure**—The physical and hardware components of a system (facilities, equipment and networks)
   - **Software**—The programs and operating software of a system (systems, applications and utilities)
   - **People**—The personnel involved in the operation and use of a system (developers, operators, users and managers)
   - **Procedures**—The automated and manual procedures involved in the operation of a system
   - **Data**—The information used and supported by a system (transaction streams, files, databases and tables)
3. The boundaries or aspects of the system covered by the Description
4. How the system captures and addresses significant events and conditions
5. The process used to prepare and deliver reports and other information to user entities and other parties
6. If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization or other parties; and the procedures performed to determine that such information and its processing, maintenance and storage are subject to appropriate controls
7. For each principle being reported on, the applicable Trust Services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user entity controls contemplated in the design of the service organization's system.
8. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable Trust Services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with our privacy commitments. For subservice organizations presented using the inclusive method, a Management Assertion and Management Representation Letter must be provided by the subservice organization.
9. Any applicable Trust Services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons why
10. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable Trust Services criteria

Example of a Written Assertion by Management of the Service Organization *(cont.)*

11. Relevant details of changes to the service organization's system during the period covered by the Description

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

b. The controls stated in Description were suitably designed throughout the specified period to meet the applicable Trust Services criteria, and the controls stated in the Description operated effectively throughout the specified period to meet the applicable Trust Services criteria.

Note that under (a)(i)(6) in the previous example, it states "for each principle being reported on," meaning that not all principles may be included within the SOC 2 report.

SOC 2 Report Section 3

Design (Type 1 and Type 2) and operating effectiveness (Type 2 only) testing results

Within the report, for each principle, the criteria and the controls in place to meet each criterion are described. Additionally, the testing details and results are documented for Type 2 reports, as shown in **figure 3**. For example:

- The service organization will perform the following to determine if controls are suitably designed:
  - Identify risk that threatens the achievement of the principle, improving understanding of risk and vulnerabilities.
  - Determine that risk will not prevent principles from being achieved if controls operate as described, which increases the understanding of the controls' impact when meeting the principle(s).

Figure 3—Unauthorized Access Tests

Principle	Criterion	Client Content Group Control	Work Performed and Deviations
The system is protected against unauthorized access (both physical and logical).	The entity's security policies include, but may not be limited to, the following matters: • Registration and authorization of new users	Internal XYZ security policies exist.	Inspected: • Information security policy No exceptions noted.

The service organization will perform the following to determine whether controls operated effectively throughout the period specified in the report, which improves the monitoring of controls:

- The controls were consistently applied as designed for the specified period.
- Manual controls were applied by individuals who have the appropriate competence and authority.

SOC 2 Report Section 4

The service auditor's expressed opinion

The criteria for each principle stated in section 1 (management's description of the service organization's system) are the criteria for the opinion. The principles have been defined by the AICPA/CICA and are selected by the service organization based on their relevance to the needs of user entities. Based on that, the service auditor will communicate within the report the results of his/her assessment by expressing an opinion on the following:

- Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period (or, in the case of a Type 1 report, as of a specific date). The report:
  - Presents how the service organization's system was designed and implemented
  - Does not omit or distort information relevant to the service organization's system
- The controls related to the criteria stated in management's description of the service organization's system were suitably designed throughout the specified period.
- The controls were consistently applied as designed and operated effectively throughout the specified period. If applicable, complementary user entity controls were consistently applied as designed and operated effectively throughout the specified period.
- If applicable, compliance with the commitments in the statement of privacy practices throughout the specified time period (when the report includes the privacy principle)

Example of a Type 2 Nonqualified Opinion

In our opinion, in all material respects, based on the Description Criteria identified in client's assertion and the applicable Trust Services criteria:

a. The description fairly presents the system that was designed and implemented throughout the period 1 January 2011 to 31 December 2011.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable Trust Services criteria would be met if the controls operated effectively throughout the period 1 January 2011 to 31 December 2011, and user entities applied the complementary user entity controls contemplated in the design of the client's controls throughout the period 1 January 2011 to 31 December 2011.

c. The controls tested, together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable Trust Services criteria were met, operated effectively throughout the period 1 January 2011 to 31 December 2011.

COBIT 5

ISACA’s COBIT 5[2] may be used by service organizations to implement management practices over the control environment. It is useful for user entities to be aware that this framework exists and may have been used to set up the control environment at a service organization.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from information technology (IT) by maintaining a balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

The COBIT 5 process reference model is shown in **figure 4** and subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes:

- Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritization and decision making; and monitoring performance, compliance and progress against agreed direction and objectives (Evaluate, Direct and Monitor [EDM]).
- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (plans, builds, runs, monitors [PBRM]).

Exercising governance and management effectively in practice requires appropriately using all enablers. The COBIT process reference model allows one to focus easily on the relevant enterprise activities.

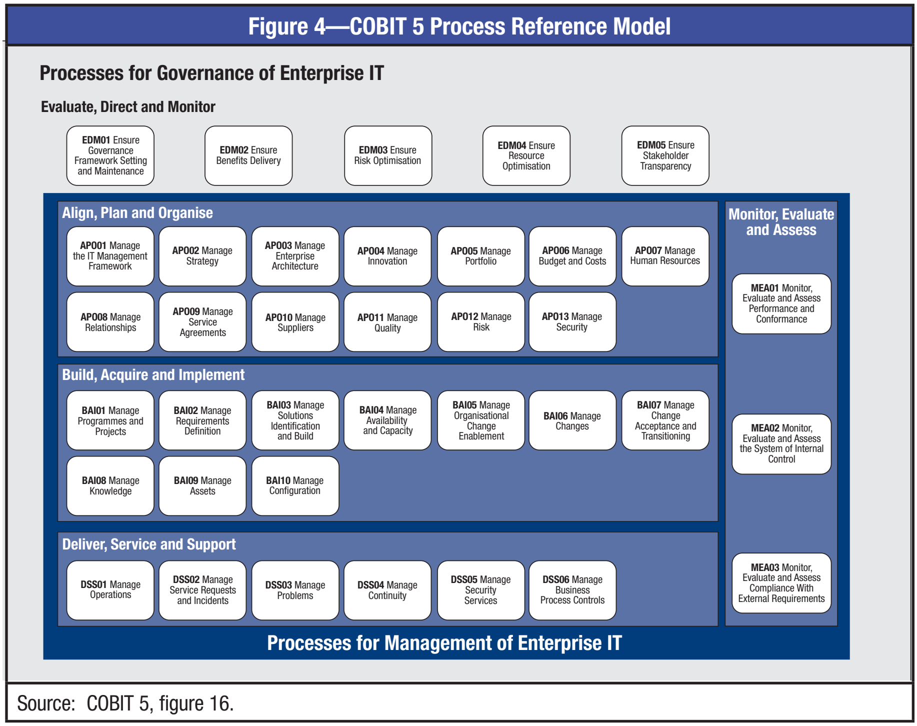
The ISACA publication *COBIT® 5: Enabling Processes* contains this process reference model, in which process internal good practices are described in growing levels of detail:

- **Practices**—For each COBIT 5 process, the governance/management practices provide a complete set of high-level requirements for effective and practical governance and management of enterprise IT.
- **Activities**—Activities are defined as “guidance to achieve management practices for successful governance and management of enterprise IT.” The COBIT 5 activities provide the how, why and what to implement for each governance or management practice to improve IT performance and/or address IT solution and service delivery risk. This material is of use to:
  - Management, service providers, end users and IT professionals who need to plan, build, run or monitor (PBRM) enterprise IT
  - Assurance professionals who may be asked for their opinions regarding current or proposed implementations or necessary improvements.

[2] ISACA, COBIT® 5, USA, 2012, *www.isaca.org/cobit*

- **Detailed activities**—The activities may not be at a sufficient level of detail for implementation, and further guidance may be needed.

Figure 4—COBIT 5 Process Reference Model



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

APO01 Manage the IT Management Framework

APO02 Manage Strategy

APO03 Manage Enterprise Architecture

APO04 Manage Innovation

APO05 Manage Portfolio

APO06 Manage Budget and Costs

APO07 Manage Human Resources

APO08 Manage Relationships

APO09 Manage Service Agreements

APO10 Manage Suppliers

APO11 Manage Quality

APO12 Manage Risk

APO13 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI10 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

Source: COBIT 5, figure 16.

In summary, COBIT 5 allows managers to bridge the gap with respect to control requirements, technical issues and business risk, and communicate that level of control to stakeholders. It enables the development of clear policies and good practice for IT control throughout enterprises.

Section 4. Evaluating the User Entity Needs

A SOC 2 report is intended to provide assurance that risk related to the processes outsourced to a service organization are addressed by effective controls. However, SOC 2 reports can vary by system covered, principles(s) covered, and the needs the user entities intended to address. For example, some user entities may need a system that can be restored in 48 hours in the event of a major outage while others may require fault-tolerant systems that can automatically failover to a second processing environment.

To assess whether a SOC 2 report will meet a user entity's particular needs, the user entity needs to identify the purpose for obtaining the report and view the report from a holistic point of view. For instance, a report requested by corporate for performance measurement for vendor management purposes has a different purpose than a report requested by the internal audit department for operational risk purposes. A report used for vendor management purposes likely focuses more on the business processes in place at the vendor site and how those processes are effectively managed by controls designed to meet the criteria applicable to the principles relevant to the user entity, specifically, evaluating the narrative and controls. On the other hand, one focus of an internal audit reviewer may be on the adherence of the controls to leverage for reporting purposes, specifically focusing on operational risk to determine how management is monitoring and/or managing the risk.

Assess the Risk for the User Entity

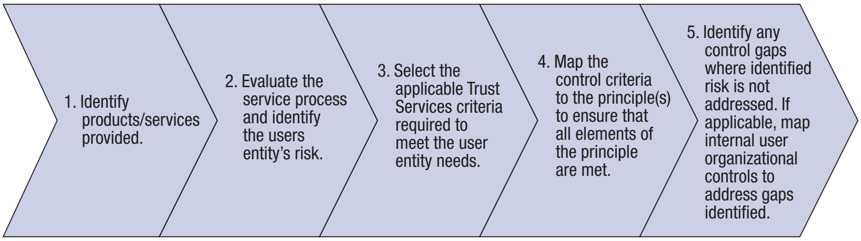
A SOC 2 report allows a user entity to understand the significant risk related to the business and gives the user entity the opportunity to see how the risk is assessed and monitored by the management of the service organization.

Significant risk needs to be identified by all impacted users of the services provided. For example, when outsourcing cloud computing, availability and user access will be identified as key business risk areas. How does the service organization ensure that the information is available to users? If users are not able to gain access to their accounts, the user entity could potentially lose customers. How does the service organization ensure that the cloud users are only granted permission to their data and not the data of other users? If other users gain unauthorized access to information and use that information maliciously, it can negatively affect the user entity's reputation.

Banks that outsource services—such as clearing and settlement—expect fraud controls to be in place to protect user data such as bank account numbers and to restrict access to unique personal identification numbers (PINs). Additionally, US banks are subject to privacy and compliance with GLBA to protect this sensitive information. Changes to this information in the IT system should be requested and approved by authorized individuals. If unauthorized access occurs or a lack of monitoring exists, it could lead to fraudulent transactions being processed at the service organization or a breach in privacy resulting in a leakage of sensitive information. Therefore, user access management is a key risk area for banks.

The assessment of each key risk to the user entity should be identified by all affected service users and should include the steps in **figure 5**.

Figure 5—Risk Assessment Steps



1. Identify products/services provided.
2. Evaluate the service process and identify the users entity's risk.
3. Select the applicable Trust Services criteria required to meet the user entity needs.
4. Map the control criteria to the principle(s) to ensure that all elements of the principle are met.
5. Identify any control gaps where identified risk is not addressed. If applicable, map internal user organizational controls to address gaps identified.

Each step is further described in the following subsections.

1. Identify Products/Services Provided

A user entity that intends to outsource all or part of its activities to a service organization must first obtain a thorough understanding of the different services provided by the service organization to make sure the services correspond to its needs. The services can be identified through the description section of the SOC 2 report, which provides details regarding the processes in place at the service organization. Because the risk is different depending on the intended use of the report, each affected user (e.g., purchasing, IT, internal audit) should evaluate the products/services provided to identify the related risk.

The user entity must gain an understanding of the key processes needed at the service organization to support the services it wants to outsource. This includes reading the SOC 2 report to understand the processes and procedures by which services are provided, including how transactions are initiated, authorized, recorded, processed, corrected and reported. The user entity needs to verify that the report includes the technology platforms, applications, systems, IT and/or business processes, locations or services that support the user entity's specific systems or outsourced operations. A well-written SOC 2 report clearly identifies the scope of what is included and not included within the report. If the report does not cover the areas or services provided that are relevant to the user entity, the usefulness of the report may be limited. In this situation, the user entity should consider the risk related to the areas not addressed in the scope and, depending on the risk, either identify and test the controls it uses to manage the service organization's effectiveness or identify and test the relevant controls performed by the service organization.

2. Evaluate the Service Process and Identify the User Entity's Risk

An end-to-end understanding of the processes at the service organization and user entity will enable the user entity to identify key risk areas and to determine whether the necessary controls have been implemented to mitigate those risk areas. The user entity should provide the specifications needed for controls at the service organization to ensure that (1) the risk is effectively addressed and (2) such controls are included in the service auditor's report.

For example, several areas of risk for the user entity exist within the user access management process. These may include terminated employees remaining active in the system, new employees gaining too much access in the system, or changes of job function within the organization (e.g., from purchasing to payables) that result in segregation of duties conflicts. Additionally, companies may be concerned with compliance risk as it relates to privacy and the protection of sensitive information. Each of these areas creates a different risk, and the user entity should expect that the service organization has principles with control criteria in place to mitigate the risk areas identified.

3. Select the Applicable Trust Services Principles and Criteria Required to Meet the User Entity Needs

The user entity should consider which Trust Services principles and criteria are most relevant to the services being provided by the service organization. After defining these requirements, the user entity must validate that the identified Trust Services principles and criteria are included accordingly in the SOC 2 report.

4. Map User Entity Control Requirements to the Applicable Trust Services Criteria Associated with the Principles to Be Included in the SOC 2 Report

In the SOC 2 report, each control addressing specific criteria is listed under the principle it supports. Criteria may have one or more controls to ensure that all parts of the principle are achieved. When mapping the controls to the criteria, it is a good technique to break down the list of requirements into sections named after the applicable principles to determine what controls should be implemented at the service organization to satisfy the necessary principles.

5. Identify Any Control Gaps Where Identified Risk Is Not Addressed—If Applicable, Map Internal User Organization Controls (Complementary Controls) to Address Gaps Identified

Once steps 1 to 4 are completed, the user entity should be able to identify any gaps that are not addressed within the report. One common overlooked area is in-house-developed data or processes impacting service organization's utilities, which can lack formalized authentication and audit trails.

Regardless whether gaps exist, the user entity should evaluate its own internal controls (especially those considered as user entity complementary controls) to determine if all identified risk are mitigated. These complementary user entity controls are a critical component of the report and illustrate to the intended user of the report that the user entity has certain roles, responsibilities and obligations in helping the service organization achieve the principles stated and, therefore, it is common to list these controls within the description in the SOC 2 report. Examples of complementary user entity controls include:

- User entity controls related to system access and acceptable use for all systems that interface with the service organization's systems (directly or indirectly)
- User entity timely deactivation or removal of user accounts for user entity terminated employees previously involved in functions or activities involving service organization's systems
- User entity timely deactivation or removal of user accounts for user entity terminated employees previously involved in functions or activities involving systems interfacing with service organization's systems
- User entity controls implemented to protect data transmitted to the service organization (appropriate methods must be implemented to ensure security, availability, integrity, confidentiality or privacy accordingly)

Please note that the term complementary "user entity controls" may also be expressed as "user organization controls," "complementary customer controls" or any other similar name or phrase that refers to controls implemented and managed by the user entity.

Page intentionally left blank

Section 5. Communicating Needs to the Service Organization

Vendor Management Focus

Vendor management enables the user entity to build a relationship with the service organization that can provide value to and strengthen both businesses. The value is created when the user entity works continually with the service organization to discuss changes and come to mutually beneficial agreements.

The user entity's sharing of information and priorities with the service organization is an important success factor for vendor management. This means that the user entity provides the necessary information to the service organization at the right time so the service organization can better meet the user entity's needs. This is important for several reasons, including scoping of the SOC 2 report so that the service organization knows what reliance is being placed on the report by the user entity and service agreements, and contracts can be negotiated appropriately.

Part of vendor management is the user entity's contribution of knowledge or resources that may help the service organization meet the user entity's needs. The user entity can approach this by querying the service organization about its side of the business. When trust is established between the user entity and the service organization, a long-term relationship can be built and both companies can benefit from the enhanced communications, improved negotiations, and greater understanding of each other's business and needs.

In many cases, a service level agreement (SLA) that outlines the services to be provided is signed between the user entity and the service organization. When the services in question are complex in nature, measuring their quality (and thus the fulfillment of the service organization's promise) becomes a challenge. In these cases, a SOC 2 report may help both parties evaluate how compliance and operational risk is controlled by the service organization.

User Entity Requirements

The user entity should identify what processes are outsourced and what operational risk arises from the performance of these processes. As a next step, the management of the user entity should outline the specifications needed of the third-party assurance reports to ensure that the risk is effectively addressed by relevant controls.

What to Ask of the Service Organization

Because communicating with the service organization is essential, the user entity should ensure that a communication strategy is established within the contract agreement. When planning to obtain a SOC 2 report, a strategy should be established by the user entity, including identification of the stakeholders (audience).

Working with the appropriate representatives, the user entity can identify the products that are being outsourced along with the associated financial or operational risk. (Section 4, Evaluating the User Entity Needs, provides details on how to perform this assessment.)

The user entity may need to ask some of the following questions to determine the type of report required to meet its needs:

- Will the scope of the system(s) covered be appropriate to the user entity needs?
- Will the principles being reported on be relevant to user entity needs?
- Will significant activities performed by subservice organizations be included or carved out?
- If significant activities will be carved out, are there other sources of information and assurance about such activities (e.g., another service-auditor report on the carved-out activities)?
- Is it likely that the opinion of the service auditor will include significant exceptions and, if so, how might these affect risk at the user entity?
- Who is going to use this report and for what purpose?
- Does the audience include auditors or others who need details about controls and test results, or will a general use report fulfill audience needs?
- What coverage period is required: point in time or over a period of time?

Negotiating the Depth of Detail Documented in the SOC 2 Report

Some user entities require very detailed and elaborate control descriptions to address high risk while other user entities may be satisfied with less. To determine the appropriate level of detail can be challenging for service organizations so it is important for the user entity to establish a relationship and communicate its needs and expectations when receiving a SOC 2 report. User entities should be cautious with service organizations that do not provide a thorough SOC 2 report and work to establish a mutually beneficial relationship where each organization's requirements can be discussed.

Some service organizations may not understand how SOC 2 reports can help their business so they may be reluctant to invest in obtaining one. A primary advantage to service organizations is the competitive advantage they obtain by applying best practice advice when implementing and reporting on their controls. A service organization that is the only company within its industry that does not provide a SOC 2 report to its users is likely to find itself at a significant competitive disadvantage.

Data privacy, security and confidentiality are increasing concerns for enterprises that collect and process certain types of data as regulators tighten the rules on data governance. User entities that are concerned with security, confidentiality and privacy are more likely to partner with service organizations that are audited by an independent auditor and can provide a SOC 2 report on the principles outlined in this guide. In addition, user entities that are concerned with availability and processing integrity are more inclined to partner with service organizations that can provide a SOC 2 report on their operational controls. Most companies are utilizing IT systems to perform their critical operations; they need to be sure that their service organizations have procedures and controls in place to provide reliable services.

An independent auditor applies industry expertise in assessing the controls in the service organization. Therefore, use of an independent auditor can provide the service organization with a better understanding of how risk is addressed in similar organizations in the same industry. Better understanding of the risk faced by clients enables the management of the service organization to steer the organization's operations to offer better services.

Page intentionally left blank

Section 6. Interpreting the Report

Type of Report (Type 1 or 2)

Is this a Type 1 or Type 2 report?

The user entity should note whether the SOC 2 report is a Type 1 or a Type 2 report. (See section 3 for an explanation of the differences between the two types of reports.) Because the scope of the service auditor's opinion is limited in a Type 1 report, a Type 2 report is generally preferable, unless the user entity wants to understand only the nature of the controls at the service organization and whether they are adequately designed. A Type 2 report is necessary if the user entity's auditor plans to use the report for reliance on internal control or the report is to be used by the user entity's management or auditor for the assessment of internal controls.

Description/Narrative Section

Why is this important to the user entity? How can it be used (e.g., gaining an understanding)? How can the user entity evaluate the depth of detail?

The user entity should determine whether the service organization has included sufficient detail in the description section of the report provided. The description should clearly detail the systems, services, transactions, reports and business processes performed at the service organization to enable the user entity to understand the structure and processes supported. The depth of detail should enable the user entity to identify risk areas where controls that address the criteria associated with each principle have been in place by the service organization. This will make it possible for the user entity to identify any design gaps within the report.

Example 1 Description That Provides Sufficient Detail Regarding Selected Monitoring in Place at XYZ Service Organization

Monitoring
XYZ management team, with support from its internal audit department, monitors the effectiveness of the company's controls over security through the performance of semiannual audits of such controls and ongoing review and testing procedures performed by management. Identified security deficiencies are generally corrected within 24 hours.

Example 2 Description That Lacks Sufficient Detail Regarding Selected Monitoring in Place at XYZ Service Organization

Monitoring
XYZ management team, with support from its internal audit department, monitors the company's system of internal control. Deficiencies in the company's system of internal control are reported to management.

In example 1, the description provides details on scope, frequency and deficiency-handling process for monitoring the service organization's system of internal control. Example 2 simply states that monitoring is performed and deficiencies are reported without providing details on the scope, frequency and full process to handle the deficiencies. As a result, example 1 is much more descriptive than example 2 and will be more useful to the user entity when evaluating the processes and controls in place at the service organization.

Management's Assertion

Why is this important to the user entity and how should it interpret this?

The service organization is required to provide a written assertion that states the scope of the report. The assertion also affirms management's responsibility for the content of the report, including the description of IT systems/business processes, principle(s) and control criteria. Specifically for the SOC 2 report, this includes the assertion by management that security, availability, processing integrity, confidentially and privacy controls are fairly presented and suitably designed (Type 1 and 2) and are operating effectively (Type 2 only) to achieve a specific principle. For privacy, specifically in a Type 2 report, the written assertion will include a statement regarding compliance with the commitments in the Statement of Privacy Practices throughout the period. This assertion is available for auditors and users of the organization's services.

The user entity should interpret management's assertion as an indication from the service organization's management that it formally takes responsibility for the SOC 2 report and its content.

Through the assertion, management communicates its responsibility for the fair presentation of the description of the organization's controls and for establishing and maintaining appropriate controls related to the processing of transactions for the user entity. It also conveys management's belief that controls are suitably designed to achieve the principle(s) specified in the description of system controls. This demonstrates management's ownership of the services provided and the underlying principle(s) and controls in place to achieve those principle(s).

Considerations Regarding Suitability of the Design of Controls

Principles

The selection of principles being reported on is strictly up to the service organization. Additionally, all criteria, unless they are deemed not relevant for the selected principles, are expected to be included in the report. The main issue that should be considered by the user entity is the following question: Are the principles selected (covered by the report) appropriate for the needs of the user entity?

For example, a report on the processing integrity principle where system processing is complete, accurate, timely and authorized is of little use to a user entity seeking assurance about privacy. The user entity would expect that a service organization requiring compliance with the commitments in its statement of privacy principles would include the Generally Accepted Privacy Principles and Criteria. Some privacy components include policies addressing the use, retention and disposal of sensitive information.

Design of Controls

A SOC 2 report identifies the control criteria designed to achieve the principles, including potential controls that the service organization intends for the user entity to implement (referred to as "complementary user entity controls"). While the specified controls should address the risk that threatens the achievement of the principle for most user entities, individual user entity needs may vary. As a result, the user entity should consider the risk that would threaten the achievement of the principle from its own perspective and consider whether the controls identified adequately address the risk. If the user entity believes that any risk areas are not addressed by the service organization's controls, the user entity should discuss those risk areas with the service organization.

Additionally, the report may include complementary user entity controls. These controls are a critical component of the report and illustrate to the intended user of the report that the user entity has certain roles, responsibilities and obligations in helping the service organization achieve the principles stated and, therefore, it is common to list these within the description for a Type 1 and Type 2 report.

Subservice Organizations

What is a subservice organization and how can it have an impact on the user entity?

A service organization may use another service organization to perform functions or processing, which can affect services provided to the user entity. For example, the data center is often outsourced to a subservice organization. There are two types of related reporting within the SOC 2 reports when using a subservice organization: carve-out and inclusive.

When the carve-out method is used, management's description of the service organization's system identifies the nature of the services and functions performed by the subservice organization and the types of controls that management expects to be implemented at the subservice organization, but excludes details of the subservice organization's system and controls. Using this method does not mean that the user entity is not required to address the controls implemented at the subservice organization. As a user entity, the monitoring controls should be evaluated to determine whether these sufficiently address the identified risk for the outsourced services. If the service organization uses the carve-out method to present a subservice organization, the description of the service organization's system identifies the following:

- The nature of the services provided by the subservice organization
- If the description addresses the privacy principle, any aspects of the personal information life cycle for which responsibility has been delegated to the subservice organization, if applicable
- Each of the applicable Trust Services criteria that are intended to be met by controls at the subservice organization alone or in combination with controls at the service organization
- The types of controls expected to be implemented at carved-out subservice organizations that are necessary to meet the applicable Trust Services criteria, either alone or in combination with controls at the service organization
- If the description addresses the privacy principle, the types of activities that the subservice organization would need to perform to comply with the service organization's privacy commitments

The description of the service organization's system and the service auditor's engagement exclude all other aspects of the subservice organization's infrastructure, software, people, procedures and data relevant to the services provided.[3]

The inclusive method is where the service organization's description of its system includes the services performed by the subservice organization as well as the applicable Trust Services criteria and related controls of the subservice organization.

When the inclusive method is used, the following is performed to produce the report:

- Obtaining acknowledgement and acceptance of responsibility for the matters from management of the subservice organization
- Obtaining an understanding of the portion of the system provided by the subservice organization
- Obtaining and evaluating evidence about the fairness of the presentation of the description for the portions of the system provided by the subservice organization
- Obtaining evidence about whether the described controls have been implemented at the subservice organization
- Evaluating the suitability of the design of controls at the subservice organization
- For a Type 2 report, obtaining evidence of the operating effectiveness of controls at the subservice organization
- Obtaining evidence of the subservice organization's compliance with the privacy commitments it has made to the service organization, if applicable
- Obtaining a written assertion that is relevant to the services provided by the subservice organization
- Obtaining written representations about the matters that are relevant to the services provided by the subservice organization

[3] AICPA, *SOC 2 Audit Guide*, USA, 2012, Section 3.29

Reporting When the Service Organization Uses the Carve-Out Method to Present a Subservice Organization[4]

Scope

We have examined the attached description titled “XYZ Service Organization’s Description of the Adaptable Cloud Computing System Throughout the Period 1 January 2011 to 31 December 2011” (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the privacy principle set forth in TSP Section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (applicable Trust Services criteria), throughout the period 1 January 2011 to 31 December 2011.

XYZ service organization uses a service organization (subservice organization) to perform certain processing of customers’ personal information. The description indicates that certain applicable Trust Services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description presents XYZ service organization’s system; its controls relevant to the applicable Trust Services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable Trust Services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization or the subservice organization’s compliance with the commitments in its statement of privacy practices.

Reporting When the Service Organization Uses the Inclusive Method to Present a Subservice Organization

Scope

We have examined the attached description titled “XYZ Service Organization’s **and ABC subservice organization’s** Description of the Adaptable Cloud Computing System Throughout the Period 1 January 2011 to 31 December 2011” (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, processing integrity, and confidentiality principles set forth in TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable Trust Services criteria), throughout the period 1 January 2011 to 31 December 2011. **ABC subservice organization is an independent service organization that provides certain computer processing services to XYZ service organization. XYZ service organization’s description includes a description of those elements of its system provided by ABC subservice organization, the controls of which help meet certain applicable Trust Services criteria.**

[4] AICPA, *SOC 2 Audit Guide*, Section 4.40

Reporting When the Service Organization Uses the Inclusive Method to Present a Subservice Organization *(cont.)*

Service organization's and subservice organization's responsibilities
XYZ service organization **and ABC subservice organization** have provided their attached assertions titled *[title of service organization's assertion]* and *[title of subservice organization assertion]*, which are based on the criteria identified in those management's assertions. XYZ service organization **and ABC subservice organization are** responsible for (1) preparing the description and the assertion***s***; (2) the completeness, accuracy and method of presentation of both the description and assertion***s***; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable Trust Services criteria and stating them in the description; and (5) designing, implementing and documenting the controls to meet the applicable Trust Services criteria.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in XYZ service organization's **and ABC subservice organization's** assertions and on the suitability of the design and operating effectiveness of the controls to meet the applicable Trust Services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable Trust Services criteria throughout the period [date] to [date].

Inherent limitations
Because of their nature and inherent limitations, controls at a service organization **or subservice organization** may not always operate effectively to meet the applicable Trust Services criteria. 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 meet the applicable Trust Services criteria is subject to the risk that the system may change or that controls at a service organization **or subservice organization** may become inadequate or fail.

Reporting When the Service Organization Uses the Inclusive Method to Present a Subservice Organization *(cont.)*

Opinion

In our opinion, in all material respects, based on the criteria identified in XYZ service organization's **and ABC subservice organization's** assertions:

a. The description fairly presents XYZ service organization's [type or name of] system **and the elements of the system provided by ABC subservice organization** that were designed and implemented throughout the period [date] to [date].

b. The controls **of XYZ service organization and ABC subservice organization** stated in the description were suitably designed to provide reasonable assurance that the applicable Trust Services criteria would be met if the controls operated effectively throughout the period [date] to [date].

c. The controls **of XYZ service organization and ABC subservice organization** that were tested, which were those necessary to provide reasonable assurance that the applicable Trust Services criteria were met, operated effectively throughout the period from [date] to [date].

Restricted use

This report and the description of tests of controls and the results thereof are intended solely for the information and use of XYZ service organization **and ABC subservice organization**; user entities of XYZ service organization's [type or name of] system; and those prospective user entities, independent auditors, and practitioners providing services to such user entities and regulators who have sufficient knowledge and understanding of:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations and other parties
- Internal control and its limitations
- Complementary user entity controls and how they interact with related controls at the service organization **and subservice organization** to meet the applicable Trust Services criteria
- The applicable Trust Services criteria
- The risks that may threaten the achievement of the applicable Trust Services criteria and how controls address that risk

This report is not intended to be, and should not be, used by anyone other than these specified parties.

The subservice organization can be a separate entity or related to the service organization. Regardless, the risk related to the control(s) residing at the subservice organization should be considered depending on the functions that each service organization performs. Appropriate monitoring of the subservice organization by the service organization should be taken into account when evaluating the overall control environment to ensure adherence to controls for the period of the report.

Use of Internal Audit Function

What does this mean and how does it affect the user entity?

The service auditor must disclose when the internal audit function's work has been used to form the service auditor's opinion. The documentation of the use of internal audit's test steps and results can be inserted in the test of controls section of the report. The service auditor should not reference the work of internal audit in the opinion section because the internal audit function is not independent of the service organization. The service auditor has sole responsibility for the opinion expressed in the service auditor's report, and accordingly, that responsibility is not reduced by the service auditor's use of the work of the internal audit function.

Example of Internal Audit's Testing and Results Documentation

The following example shows how the service auditor would document the use of internal audit's work within the SOC 2 report. This allows the user entity the ability to easily identify the work that is being performed by the company's internal audit team.

Internal audit inquired with:
- Network management about the monitoring on accuracy and timeliness of the reporting

Internal audit inspected:
- Sample of SLAs and verified whether key performance indicators (KPIs) for reporting were defined and how they were set up
- Sample of monthly, quarterly and annually generated KPI reports and verified that the KPIs were monitored as defined

This reporting provides transparency to the user entity and allows the user entity to identify which controls are tested by the service organization's internal audit department.

Evaluating Service Auditors' Testing

Sufficiency of Description of Test

The test description should describe the nature, timing and extent of the testing performed. The following should also be considered when evaluating the sufficiency of the description of tests performed:
- The scope of the work is appropriate to meet the principles.
- All aspects of the control description are appropriately tested and documented in the test procedures.
- Conclusions are appropriate in the circumstances.
- Reports are consistent with the results of the work performed.

Nature of Tests

The higher and more pervasive the risk relating to a given Trust Services criterion, the greater the need for assurance on relevant preventive and detective controls to meet the relevant Trust Services criteria and the more likely the control is assessed with greater significance. Several factors, including the existence of other complementary, compensating or redundant controls may be considered to determine the significant level of a control. This means that the multiple controls that are necessary to meet the Trust Services criteria will be tested for design (Type 1 and Type 2) and operating effectiveness (Type 2 only).

There are several ways to test a control: inquiry, examination, observation and re-performance. The nature of the test to be performed depends on the level of comfort required and the history of the control's performance. Therefore, the extent and the nature of the tests performed should be evaluated to ensure that they provide the right level of assurance that the controls are designed and operating effectively to meet the principle(s).

Controls are tested through:

- **Inquiry**—Involves asking about controls, which provides the auditor with some relevant information. However, inquiry of service organization personnel alone does not provide sufficient audit evidence to support a conclusion about the effectiveness of a control. Further support is needed to determine whether controls are effective; methods include examining reports, manuals or other documents used in or generated by the performance of the control or re-performing a control.
- **Observation**—An appropriate way to obtain evidence if there is no documentation of the operation of a control, such as physical controls (e.g., seeing that the warehouse door is locked or blank checks are safeguarded). Generally, evidence obtained directly, such as through observation, provides more assurance than that obtained indirectly or by inference, such as through inquiry. Observation is another way to assess the environmental risk associated with availability. Quite often service organizations and data vaulting firms are located in industrial areas that may be populated by neighbors using various chemicals that prove to be toxic in fires or are released inadvertently, etc. Such observations may require either the service organization or subservice organization to reassess availability risk from a business continuity perspective (e.g., in case of fire).
- **Examination or inspection of evidence**—Often used to determine whether manual controls, such as following up on backup failures, are being performed. Evidence may include written explanations, checkmarks or other indications of documented follow-up. This includes examining evidence of the performance of a control when it might reasonably be expected to exist.
- **Re-performance**—Generally provides better evidence than the other techniques and, therefore, is used when a combination of inquiry, observation and examination of evidence does not provide sufficient assurance that a control is operating effectively.

The nature, timing and extent of the procedures to evaluate the design or operating effectiveness should be included in the report. The following should be considered when evaluating the report:

- Whether the control as designed meets the criteria
- Timeliness of the control procedures
- Rigor and precision at which the control is designed to operate
- The period covered in the SOC 2 report—This should be the same period that the user entity is relying on for the test results.
- Timing of the of the tests performed by the service auditor
- Test of compliance with privacy commitments
- Evaluation of the use of internal audit's work

The service auditor designs tests of controls to meet the needs of the typical user entity; however, professional opinions may vary on the sufficiency of tests of controls. The user entity should also focus on the key controls that meet the Trust Services criteria and consider whether the tests performed by the service auditor are sufficient to evaluate the effectiveness of those controls. Certain control testing techniques inherently provide more assurance. For example, re-performance of a control generally provides more assurance than inquiry and observation provide. Independent tests of controls by the service auditor provide more independence and objectivity than tests performed by the internal audit function, on which the service auditor may choose to rely. Any questions on the sufficiency of testing should be addressed with the service organization.

Deviations/Observations

What are deviations and how does the user entity evaluate them (e.g., context behind them)?

SOC 2 reports include results of tests so user entitys can perform separate evaluations of the impact of control deviations on the user entity's environment. As noted previously, this is done because it is understood that the needs of user entities differ. In evaluating the reported deviations, user entities should consider the importance of the control meeting the criteria. To assist the user entity in this evaluation, the service organization or the service auditor may disclose compensating controls or mitigating factors that would reduce the impact of the deviations. If compensating or mitigating controls are provided, the user entity should consider the strength of those controls and whether the compensating or mitigating controls were tested in the report.

A deviation is reported when the control is not designed or operating effectively. The description of a control deviation included in the SOC 2 report should include the following:

- The size of the sample, when sampling has been used
- The number of exceptions noted
- The nature of the deviation

Example of a Deviation Included in the SOC 2 Report[5]

The following example illustrates the documentation of tests of controls for which deviations have been identified. It is assumed that, in each situation, other relevant controls and tests of controls would also be described:

- **Criteria**—Procedures exist to restrict physical access to the defined system, including, but not limited to, facilities; backup media; and other system components, such as firewalls, routers and servers.
- **Example service organization's controls**—Security personnel deactivate physical security access cards of terminated employees on a daily basis using a list generated by the human resources (HR) system.
- **Service auditor's tests of controls**—The auditor selected a sample of terminated employees from a list generated by the HR system and compared the termination date with the access card deactivation date for each employee.
- **Results of tests of controls**—For one terminated employee in an initial sample of 25, the employee's physical access security card was not deactivated until 90 days after the employee's last day of work. In an additional sample of 15 terminated employees, no additional deviations were noted.
- **Management's response**—The terminated employee's name was not listed on the report from the HR system until 90 days after termination. Subsequent investigation determined that the report used for removing physical access was generated based on the last payroll date of the employee, rather than the last date employed. This employee was one of 15 employees who were a part of a reduction in force and received the severance benefit. These employees each continued on the payroll system for 90 days after termination. The physical access cards of all employees receiving severance have been deactivated, and the report from the HR system has been changed to generate the list based on the last date of employment.

The user entity should evaluate the severity of all identified control deficiencies applicable to services being provided and consider potential implications with regard to the effectiveness of other controls (e.g., the company's IT general controls and other components when the deviation relates to control activities).

There are three types of deviations to consider:

- Design deviation is applicable to both Type 1 and Type 2 reports. A deficiency in design exists when (a) a control necessary to meet the criteria is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the criteria would not be met.
- Operating effectiveness deviation is applicable to a Type 2 report only. A deficiency in operation exists when a properly designed control does not operate as designed or when the person performing the control does not possess the necessary authority or competence to perform the control effectively. User entity may be required to implement controls within the organization to compensate for the control deficiency in the service organization.

[5] AICPA

- Within a privacy report there can be a compliance deviation (e.g., a failure to comply with one or more commitments in the service organization's statement of privacy practices).

Example Design Deviation[6]

The following example of an explanatory paragraph could be added to the service auditor's report, preceding the opinion paragraph, if the service auditor concludes that controls are not suitably designed to meet an applicable Trust Services criterion.

The accompanying description of ABC service organization's system states on page 8 that ABC service organization's system supervisor makes changes to the systems only if the changes are authorized, tested and documented. The procedures, however, do not include a requirement for approval of the change before the change is placed into operation. As a result, the controls are not suitably designed to meet the following criterion: Controls provide reasonable assurance that only authorized, tested and documented changes are made to the system.

The following questions should be considered when evaluating the impact on the user entity (this list is not intended to be exhaustive):

- Are there any compensating controls at either the user entity or service organization?
- Were the criteria met?
- What were the nature, timing and extent of testing?
- Was the deviation remediated during the period under review?
- Is/was management taking action to address the deviation?
- How many deviations were noted and what was the nature?
- Do the nature and frequency of the deviations indicate other potential risk, such as a lax control environment or ineffective monitoring?

Deviations should be discussed with the service organization and consideration given to adding controls and performing more testing. The value of compliance and the potential cost saving would be beneficial to both organizations.

What Is the Auditor's Opinion?

A SOC 2 report can be issued with a nonqualified (clean) opinion or qualified (deviations noted) opinion.

A qualified opinion means that the presentation of management's description of the service organization's system was not fair and/or the design and operating effectiveness of the controls to meet the applicable Trust Services criteria was not suitable and/or when the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices was incompliant, based on the service auditor's examination.

[6] AICPA

This may mean that the user entity or its auditor should not place reliance on the controls supporting a particular area at the service organization. Depending on the risk assessment performed, the user entity auditor may consider performing his/her own testing at the service organization, if the service organization failed to correct the deviations noted within the report and the qualified opinion remained unchanged; or the user entity may request a memo from the service organization detailing the corrective action taken.

Qualified Opinion Description[7]

In our opinion, *because of the matter referred to in the preceding paragraph*, in all material respects and based on criteria described in [name of service organization's] assertion on page [xx]:

- The description *does not* fairly present the [type or name of system] that was designed and implemented throughout the period.
- The controls related to **meet the applicable Trust Services criteria** stated in the description were *not* suitably designed to provide reasonable assurance that the **applicable Trust Services criteria** would be met if the control operated effectively throughout the period [date] to [date].
- The controls tested, which were those necessary to provide reasonable assurance that the **applicable Trust Services criteria** stated in the description were achieved, *did not* operate effectively throughout the period from [date] to [date].
- **If the report addresses the privacy principle, the** controls tested, which were those necessary to provide reasonable assurance of the **service organization's compliance with the commitments in its statement of privacy practices** stated in the description were *not* met throughout the period from [date] to [date].

A nonqualified (clean) opinion expresses an opinion on the fairness of the presentation of management's description of the service organization's system; the suitability of the design and operating effectiveness of the controls to meet the applicable Trust Services criteria; and when the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices, based on the service auditor's examination. A clean opinion does not mean that no deviations were noted for some controls. However, it does mean that other compensating controls were in place and tested to conclude on the opinion expressed by the service auditor.

[7] AICPA

Nonqualified Opinion Description

In our opinion, in all material respects, based on the description criteria identified in [client]'s assertion and the applicable Trust Services criteria:

- The description fairly presents the system that was designed and implemented throughout the period from [date] to [date].
- The controls stated in the description were suitably designed to provide reasonable assurance that the applicable Trust Services criteria would be met if the controls operated effectively throughout the period [date] to [date], and user entities applied the complementary user entity controls contemplated in the design of [client]'s controls throughout the period from [date] to [date].
- The controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable Trust Services criteria were met, operated effectively throughout the period [date] to [date].
- If the report addresses the privacy principle, the service organization complied with the commitments in its Statement of Privicy Practices throughout the period.

If the service organization has a qualified opinion, the following questions should be considered to evaluate the impact on the user entity (this list is not intended to be exhaustive):

- Are there any compensating controls at either the user entity or service organization?
- What were the nature, timing and extent of testing?
- Was the deviation remediated during the period under review? If so, how long was the deviation in place?
- Is/was management taking action to address the deviation?
- How many deviations were noted and what was the nature?
- What period is affected?

Subsequent Events

What is a subsequent event and why is it important to the user entity?

Subsequent events are those events that occur after the "period end date" and prior to the issuance of the final report. For example, if the "period end date" is 31 December 2011 and the report issuance date is 1 March 2012, an event that occurred on 29 February 2012 that affected the report would be considered a subsequent event. Disclosure of that event is required.

The service organization may wish to disclose such events in a separate section of the description of the service organization's system; the disclosure may be titled, for example, "Other Information Provided by the Service Organization." In a format similar to the description, this section will describe what has occurred since the "period end date."

Examples of Subsequent Events

Example events that may require disclosure to user entities are:

- Purchase of a business
- Loss of data center as a result of fire or flood
- Loss of client data affecting privacy

There may also be situations in which the event discovered subsequent to the period covered by management's description of the service organization's system up to the date of the service auditor's report would likely have *no* effect on management's assertion because the underlying situation did not occur or exist until after the period covered by management's description of the service organization's system; however, the matter may be sufficiently important for disclosure by management in its description and, potentially, the service auditor in an emphasis paragraph of the service auditor's report.

The following are examples of such subsequent events:

- The service organization was acquired by another entity. This may affect the user entity and should be considered as the transfer of controls over the outsourced services is evaluated.
- The service organization experienced a significant operating disruption. The user entity should evaluate if there was an impact to the operation of its outsourced services and consider if additional controls should be in place to prevent a future occurrence.
- A data center hosting service organization that provides applications and technology that enable user entities to perform essential business functions made significant changes to its information systems, including a system conversion or significant outsourcing of operations. The user entity should consider what operations were changed and if this affected any controls either at the service organization or complementary user entity controls.

Page intentionally left blank

Glossary

Applicable Trust Services criteria	The criteria in TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, that are applicable to the principle(s) being reported
Assurance	An objective examination of evidence for the purpose of providing the reader or user of the report with a level of comfort that security goals have been adequately met through the organization's risk management and governance processes
Boundaries of the system	The specific aspects of a service organization's infrastructure, software, people, procedures and data necessary to provide its services. When the systems for multiple services share aspects, infrastructure, software, people, procedures and data, the systems will overlap, but the boundaries of each service's system will differ. In a SOC 2 engagement that addresses the privacy principle, the system boundaries cover, at a minimum, all of the system components as they relate to the personal information life cycle within well-defined processes and informal *ad hoc* procedures.
Business continuity plan (BCP)	A plan used by an enterprise to respond to disruption of critical business processes. It depends on the contingency plan for restoration of critical systems.
Carve-out method	A method of addressing the services provided by a subservice organization, whereby management's description of the service organization's system identifies the nature of the services performed by the subservice organization and excludes from the description (and scope of the service auditor's engagement) the subservice organization's controls to meet the applicable Trust Services criteria. The description of the service organization's system and the scope of the engagement include controls at the service organization that monitor the effectiveness of controls at the subservice organization, which may include the service organization's review of a service auditor's report on controls at the subservice organization.

COBIT	A complete, internationally accepted framework for governing and manageing enterprise IT that supports enterprise executives and management in their definition and achievement of business goals and related IT goals. COBIT, published by ISACA, describes five principles and seven enablers that support enterprises in the development, implementation and continuous improvement and monitoring of good IT-related governance and management practices.
Compensating control	An internal control that reduces the risk of an existing or potential control weakness resulting in errors and omissions
Complementary user entity controls	Controls that management assumes, in the design of the service provided by the service organization, will be implemented by user entities and that, if necessary to meet the applicable Trust Services criteria, are identified as such in that description
Compliance risk	The potential threat to the earnings or businesses of a company resulting from violations or infringement of laws, regulations or stipulated practices and standards within the company, industry and government
Control weakness	A deficiency in the design or operation of a control procedure. Control weaknesses can potentially result in risk relevant to the area of activity not being reduced to an acceptable level (relevant risk threatens achievement of the objectives relevant to the area of activity being examined). Control weaknesses can be material when the design or operation of one or more control procedures does not reduce to a relatively low level the risk that misstatements caused by illegal acts or irregularities may occur but not be detected by the related control procedures.
Controls at a service organization	The policies and procedures at a service organization that are likely to be relevant to user entities' internal control as they relate to meeting the applicable Trust Services criteria. These policies and procedures are designed, implemented and documented by the service organization to provide reasonable assurance about meeting the applicable Trust Services criteria.
Controls at a subservice organization	The policies and procedures at a subservice organization that are likely to be relevant to user entities of the service organization as they relate to meeting the applicable Trust Services criteria. These policies and procedures are designed, implemented and documented by the subservice organization to provide reasonable assurance about meeting the applicable Trust Services criteria.

Criteria	The standards and benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter
Data subjects	The individuals about whom personal information is collected
Detective control	A control that detects and reports when errors, omissions and unauthorized uses or entries occur
GRC	The umbrella term covering an organization's approach across the governance, risk management and compliance areas
Inclusive method	A method of addressing the services provided by a subservice organization, whereby the service organization's description of its system includes a description of the nature of the services provided by the subservice organization as well as the subservice organization's controls to meet the applicable Trust Services criteria
Management's assertion	A written assertion by management of a service organization or management of a subservice organization, if applicable
Operational risk	A risk arising from execution of a company's business functions
Personal information life cycle	The collection, use, retention, disclosure, disposal or anonymization of personal information within well-defined processes and informal *ad hoc* procedures
Preventive control	An internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product
Privacy notice	A written communication from an entity that collects personal information to the individuals about whom personal information is collected about the entity's (a) policies regarding the nature of the information that it will collect and how that information will be used, retained, disclosed, and disposed of or anonymized, and (b) the entity's commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information; the choices that individuals have related to their personal information; the security of such information; and how individuals can contact the entity with inquiries, complaints and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

Reasonable assurance	A high, but not absolute, level of assurance
Segregation of duties	A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets
Service auditor	A qualified auditor who reports on the fairness of the presentation of a service organization’s description of its system; the suitability of the design of controls included in the description; and, in a Type 2 report, the operating effectiveness of those controls to meet the applicable Trust Services criteria. When the report addresses the privacy principle, the service auditor also reports on the service organization’s compliance with the commitments in its statement of privacy practices.
Service organization	An organization or segment of an organization that provides services to user entities related to the applicable Trust Services criteria
Statement of privacy practices	A written communication from the service organization to user entities that includes the same types of privacy policies and commitments that are included in a privacy notice (see Privacy notice). It is written from the perspective of the service organization and is provided to user entities when the service organization is involved in any of the phases of the personal information life cycle, and the user entity, rather than the service organization, is responsible for providing the privacy notice. A statement of privacy practices provides a basis for user entities to prepare a privacy notice to be sent to individuals or for ensuring that the service organization has appropriate practices for meeting the existing privacy commitments of user entities. The criteria for the content of a statement of privacy practices are set forth in the 2012 SOC 2 Audit Guide paragraph 1.35e.
Subservice provider	A service organization used by another service organization to perform services related to the applicable Trust Services criteria
Test of controls	A procedure designed to evaluate the operating effectiveness of controls in meeting the applicable Trust Services criteria. These tests may include network vulnerability or penetration testing to assess effectiveness of network controls, or (web) application security tests for vulnerabilities such as cross site scripting, cross site referencing, SQL injection, etc.

Tests of compliance with commitments in the statement of privacy practices	Procedures designed to help provide reasonable assurance of detecting material incompliance with the service organization's commitments related to privacy
Third-party review	An independent audit of the control structure of a service organization, such as a service bureau, with the objective of providing assurance to the users of the service organization that the internal control structure is adequate, effective and sound
User entity	An entity that uses a service organization

Page intentionally left blank