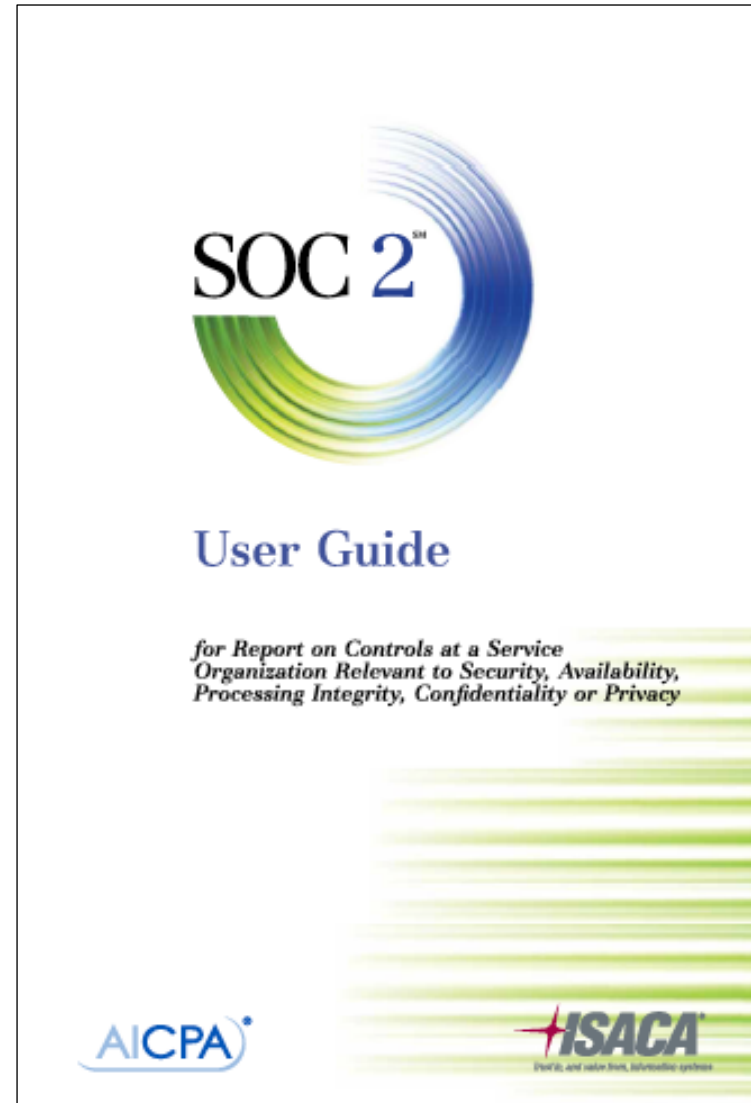


SOC 2 / SOC 3

Service Organization Control report

Round table 3 November 2014

What it is about



What you can expect

IFAC assurance reports
ISAE 3402 / SOC 1
SOC 2
SOC 3
ISACA en SOC 2 / SOC 3

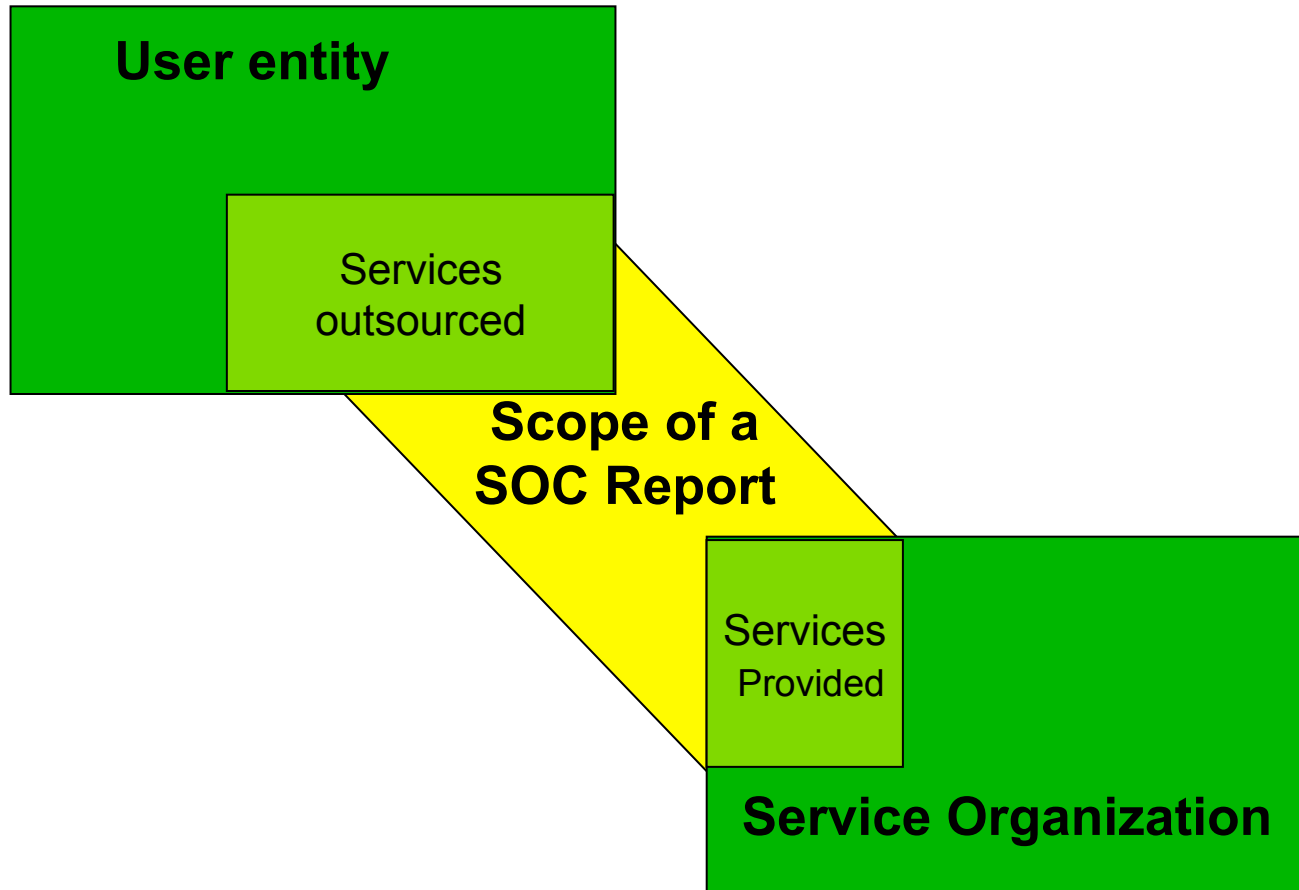
Assurance reports

- ISACA
 - ITAF (IT assurance framework)
- AICPA
 - US GAAS
- Accountants rest of the world
 - IFAC, IAASB*), ISAE standards

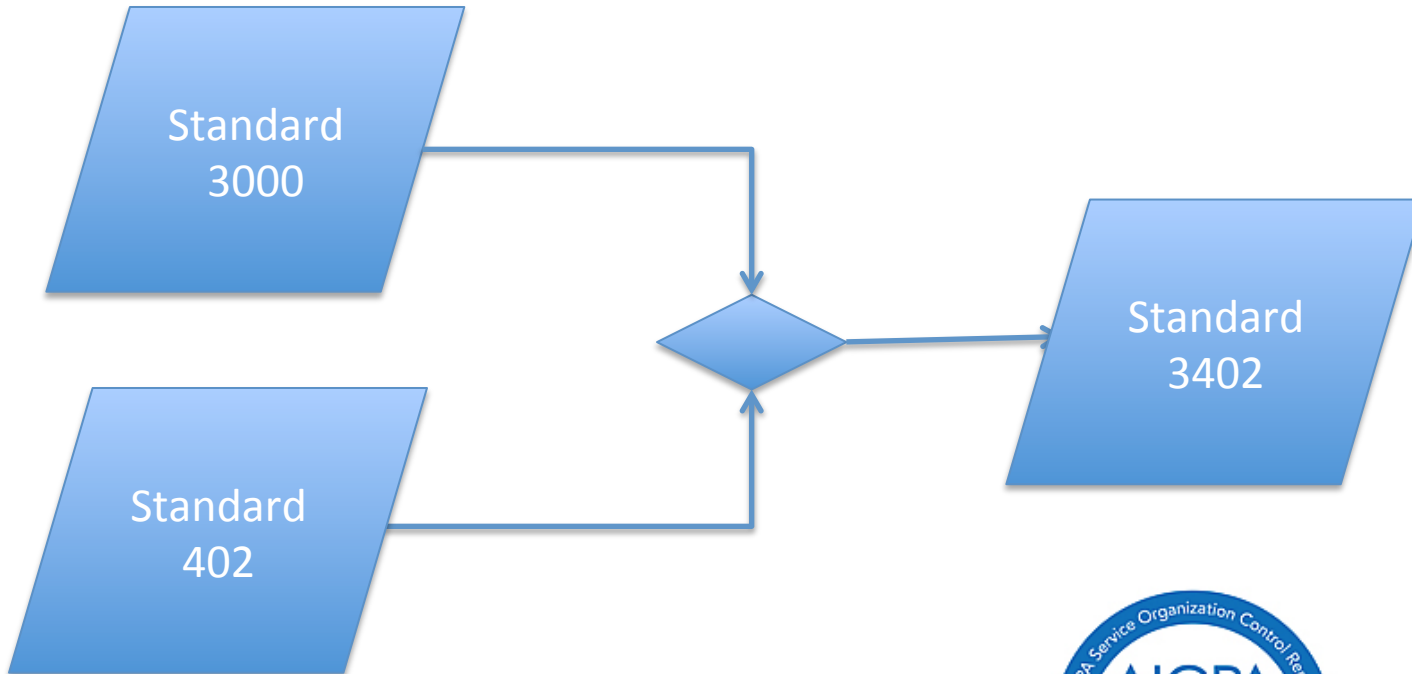


*) International Auditing and Assurance Standards Board

Assurance regarding Service Organizations



Standard 3402 / SOC 1



AICPA service organization logo

**INTERNATIONAL STANDARD ON ASSURANCE
ENGAGEMENTS (ISAE) 3402**

**ASSURANCE REPORTS ON CONTROLS AT A
SERVICE ORGANIZATION**

(Effective for service auditors' assurance reports covering periods ending on or after
June 15, 2011)

3. This ISAE applies only when the service organization is responsible for, or otherwise able to make an assertion about, the suitable design of controls. This ISAE does not deal with assurance engagements:

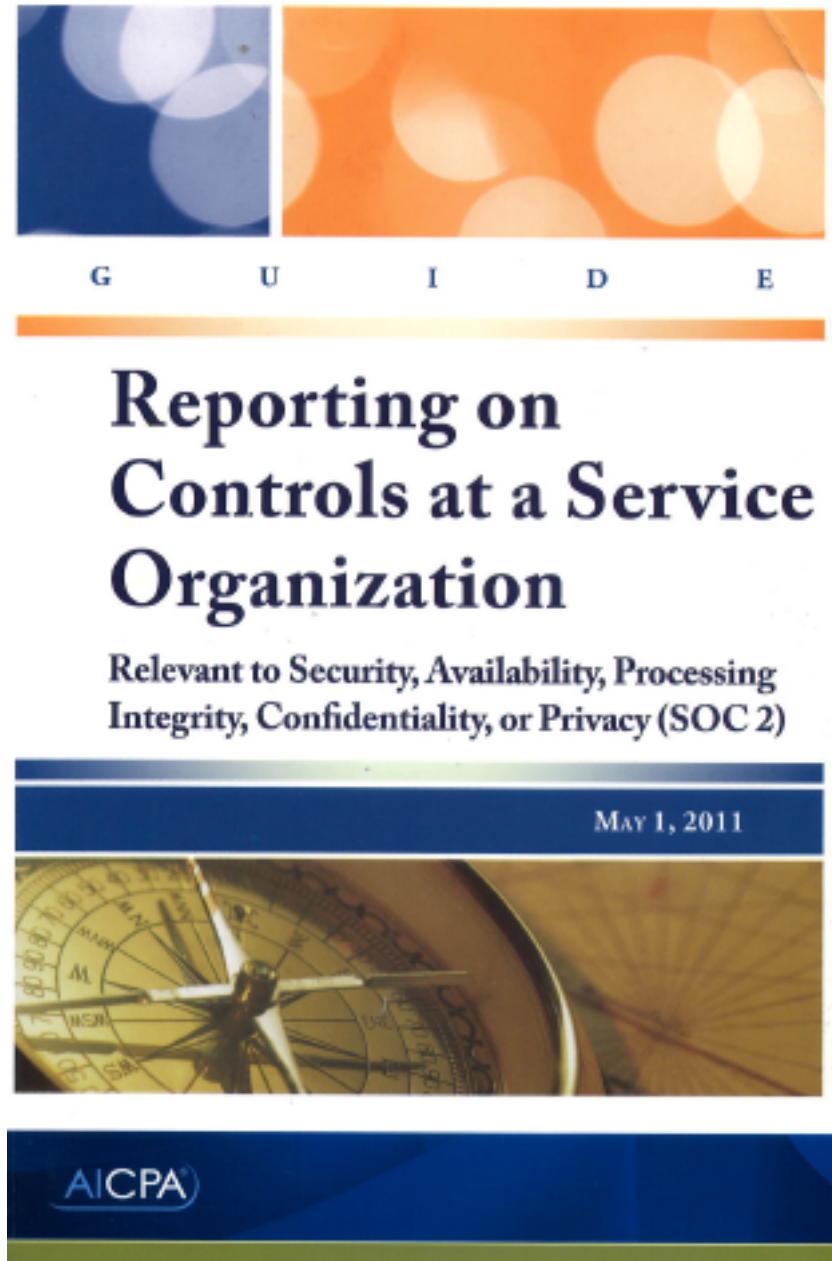
- (a) To report only on whether controls at a service organization operated as described, or
- (b) To report on controls at a service organization other than those related to a service that is likely to be relevant to user entities' internal control as it relates to financial reporting (for example, controls that affect user entities' production or quality control).

IT Service organization

This ISAE, however, provides some guidance for such engagements carried out under ISAE 3000.

Answer AICPA for IT Service Organizations: SOC 2

Based on US attestation
standard AT 101 and
Trust Services Principles and
Criteria



Trust Services principles for SOC 2 and SOC 3

Common Security Criteria		
<ul style="list-style-type: none">■ Organization and management■ Communications■ Risk Management and Design and Implementation of Controls	<ul style="list-style-type: none">■ Monitoring of Controls■ Logical and Physical Access Controls■ System Operations■ Change Management	
Availability	Confidentiality	Processing Integrity
<ul style="list-style-type: none">■ Accessibility of the system as committed by contract, SLA, or other agreements	<ul style="list-style-type: none">■ Protect of confidential information in accordance with the organization's commitments and requirements	<ul style="list-style-type: none">■ Completeness validity, accuracy, timeliness, and authorization of system processing

Privacy
<ul style="list-style-type: none">■ In US and Europe under construction

- The Trust Services Criteria (excluding Privacy) were updated in February 2014.
- Effective for periods ending on or after 15 December 2014.

Trust services criteria

components in scope of the criteria

Infrastructure, physical IT structures

Software, application and IT system software

People, personnel involved in governance, operation and use

Processes, automated and manual

Data, transactions, files, databases

Type 1

Design and
implementation

Type 2

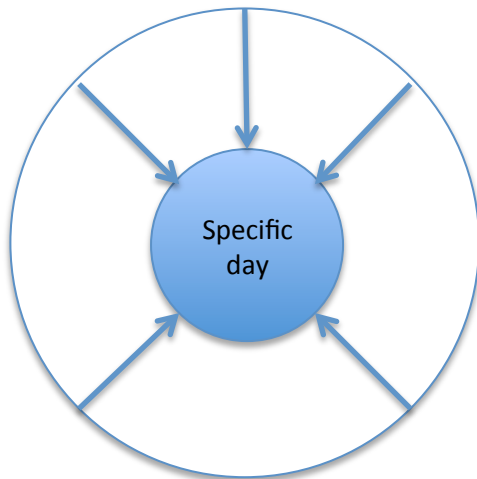
Design and
operational
effectiveness

principle	Number of criteria
Security	28 common criteria
Availability	28 common + 3 additional
Processing Integrity	28 common + 6 additional
Continuity	28 common + 6 additional
Privacy	under construction

Test work done by the auditor

Type 1

- Inquiry
- Inspection
- Observation



Type 2

- Inquiry
- Inspection
- Observation
- Re-performance

For SOC 2 / 3 minimum period of operating effectiveness not defined

Illustration of common criteria CC6.0

Criteria		Risks	Illustrative Controls
			administration personnel.
CC6.0	<i>Common Criteria Related to System Operations</i>		
CC6.1	Vulnerabilities of system components to <i>[insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof]</i> breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.	Vulnerabilities that could lead to a breach or incident are not detected in a timely manner.	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities, resource utilization, and to detect unusual system activity or service requests. This software sends a message to the operations center and security organization and automatically opens a priority incident or problem ticket and change management system record item.
			Call center personnel receive telephone and e-mail requests for support, which may include requests to reset user passwords or notify entity personnel of potential breaches and incidents. Call center personnel follow defined protocols for recording, resolving, and escalating received requests.
		Security or other system configuration information is corrupted or otherwise destroyed, preventing the system from functioning as designed.	Weekly full-system and daily incremental backups are performed using an automated system.
CC6.2	<i>[Insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof]</i> incidents, including logical and physical security breaches, failures, concerns, and other complaints are identified, reported to appropriate personnel, and acted on in accordance with established	Breaches and incidents are not identified, prioritized, or evaluated for effects.	Operations personnel follow defined protocols for evaluating reported events. Security related events are assigned to the security group for evaluation

SOC 2 Report Structure

Report structure
Auditor's Opinion
Management Assertion
Description of system and entity level controls
Criteria + Controls, tests of operating effectiveness and results of tests
Other Information
Restricted use

Section 1 — Management of Example Cloud Service Organization's Assertion Regarding its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1

Section 2 — Independent Service Auditor's Report

Section 3 — Example Cloud Service Organization's Description of its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1

System Overview and Background

Infrastructure
Software
People
Procedures
Data

Customer Responsibilities

- A. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring
 - B. Policies and Procedures
 - C. Communication
 - D. Physical Security
 - E. Logical Security
 - F. Monitoring
 - G. Relationship between CCM Criteria, Description Sections, and Trust Services Criteria
-

Section 4 — Applicable Trust Services Principles, Criteria, and CCM Criteria and Related Controls, Tests of Controls, and Results of Tests

Section 5 — Other Information Provided by Example Cloud Service Organization Not Covered by the Service Auditor's Report



CSA Position Paper on AICPA Service Organization Control ReportsSM

February 2013



Illustrative Type 2 SOC 2SM Report with the Criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)



The AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2SM)* specifies the components of a SOC 2SM report and the information to be included in each component, but it does not specify the format for these reports. Service organizations and service auditors may organize and present the required information in a variety of formats. The format of the illustrative type 2 SOC 2 report presented in this document is meant to be illustrative rather than prescriptive. The illustrative report contains all of the components of a type 2 SOC 2 report; however, for brevity, it does not include everything that might be described in a type 2 SOC 2 report. Ellipses (...) or notes to readers indicate places where detail has been omitted.

The trust services principle(s) being reported, the controls specified by the service organization, and the tests performed by the service auditor are presented for illustrative purposes only. They are not intended to represent the principles that would be addressed in every type 2 SOC 2 engagement, or the controls, or tests of controls, that would be appropriate for all service organizations. The trust services principles on which the report is based, the controls a service organization would include in its description, and the tests of controls a service auditor would perform for a specific type 2 SOC 2 engagement will vary based on the specific facts and circumstances of the engagement. Accordingly, it is expected that actual type 2 SOC 2 reports will address different principles and include different controls and tests of controls that are tailored to the service organization that is the subject of the engagement.

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Version 1.4 is used for the purpose of this illustrative report. The CSA periodically issues new criteria. The practitioner should identify the CCM version being used as criteria in management's assertion and the service auditor's report.

Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2009) is used for the purpose of this illustrative report. The AICPA periodically issues new *Trust Services Principles and Criteria*. The practitioner should identify the current *Trust Services Principles and Criteria* version for management's assertion and the service auditor's report.

aicpa.org/FRC

CCMv3 [®]		CLOUD CONTROLS MATRIX VERSION 3.0		
Control Domain	CCM V3.0 Control ID	Control Specification	Phys	
			Phys	Network
Application & Interface Security Application Security	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.		X

SOC 2 User Guide



Download (813K; Free to Members Only)



Purchase the E-book



Purchase the Book



Provide feedback on this document

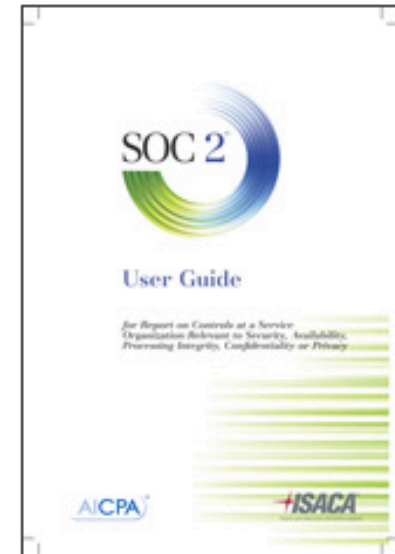


Visit the Service Management Knowledge Center community

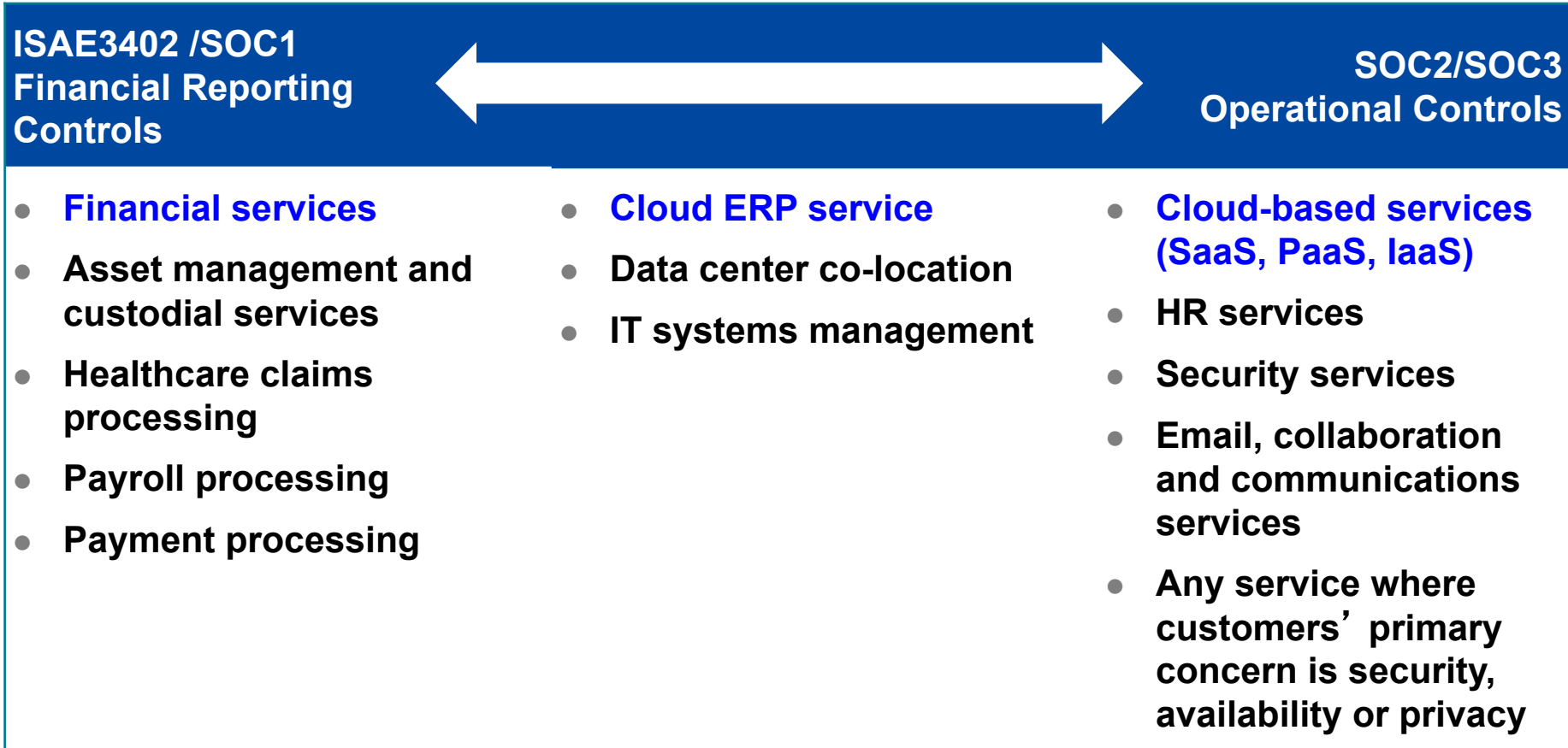
SOC 2 is a *Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*. This guide is intended for those evaluating a service organization's SOC 2 report as part of a governance, risk and compliance (GRC) program; vendor assessment; security evaluation; business continuity plan 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

AICPA and ISACA have jointly released this guide to provide user entities with the information they need when interpreting the SOC 2 reports received from service organizations. This guide also complements the companion white paper titled *New Service Auditor Standard: A User Entity Perspective* available at www.isaca.org/service-auditor-standard.



SOC Reports for Different Scenarios



SOC 3

- Based on Trust Service Principles and Criteria.
- Short form report.
- For general use / distribution.
- Carve out of subservice provider(s) not permitted.
- Modified Opinion not allowed.



Source: <https://www.dropboxatwork.com/tag/security/>

SOC 2 / SOC 3 Report Comparison

SOC 2

Includes detail on the service provider's controls, the auditor's detailed test procedures and the test results of those tests

The report enables the reader to assess the service provider at a more granular level


SOC 3

Provides an overall conclusion on whether the service provider achieved the stated Trust Services Principle

Where the service detail and description of tests of controls and results are not needed by report users or where service providers may not be willing to share a detailed report

Recap

Service Organization Control Reports

Report	Scope/Focus	Summary	Applicability	Standard
Standard 3402 / SOC1^{1M}	Internal Control Over Financial Reporting	Detailed report for customers and their auditors	<ul style="list-style-type: none"> ■ Focused on financial reporting risks and controls specified by the service provider. ■ Most applicable when the service provider performs financial transaction processing or supports transaction processing systems. 	ISAE 3402 / AT 101
SOC2SM	Security, Availability, Processing Integrity, Confidentiality and/or Privacy	Detailed report for customers and specified parties	<ul style="list-style-type: none"> ■ Focused on Security, Confidentiality, Availability, Processing Integrity and/or Privacy. ■ Applicable to a broad variety of systems. 	AT 101 / ISAE 3000
SOC3SM	Same as SOC2 SM 	Short report that can be generally distributed, with the option of displaying a web site seal	<ul style="list-style-type: none"> ■ Same as above without disclosing detailed controls and testing. ■ Optionally, the service provider can post a Seal if they receive an unqualified opinion. 	AT 101 / ISAE 3000

Objective achieved?



Responsibilities

A photograph of a beach with waves and a rainbow in the sky. The rainbow is prominent, arching over the ocean. The beach is sandy and the waves are breaking onto the shore.

Email: han@hanboer.nl
Tel: 0651261402

These slides are intended solely for participants in the ISACA Netherlands round table of 3 November 2014 to support the explanations given and may not be used for other purposes.