ControlCase
Compliance as a Service

AICPA
Service Organization Control Reports
(SOC 1, SOC 2, SOC 3)

Agenda

- Risk and Challenges
- Understanding SOC 1, 2, 3 reports
- Type of Reports
- SOC 2 Trust Services Principles
- SOC 1 COSO Framework

ControlCase
Compliance as a Service

Cybersecurity risk and challenges

- The news stories abound: from malware attacks to executive impersonation, cybersecurity-related incidents are on the rise. Every individual, every company – regardless of size – is at risk. According to Juniper Research, the costs are expected to increase to more than $2 trillion by 2019.
  - Nearly 60% of anticipated data breaches worldwide will occur in North America, but this proportion will decrease over time as other countries become both richer and more digitized.
  - The average cost of a data breach will exceed $150 million by 2020, as more business infrastructure gets connected.
- In 2015, 43% of cyberattacks were aimed at small businesses, according to Symantec.
- Cloud computing has ushered in an era of broader collaboration. But making data more available to employees, partners and clients introduces risk. The best way to mitigate that risk is to understand cloud computing options and prepare for possible breaches.

ControlCase
Compliance as a Service

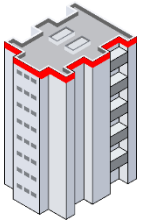
Governance and SOC reports

AICPA Building a Foundation for CPAs in Cybersecurity Risk Management

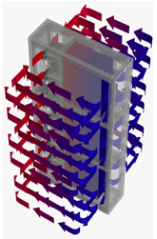
With cybersecurity threats (hacks, breaches or phishing scams) proliferating, organizations are under increased pressure to communicate with key stakeholders on the cybersecurity risk management programs they have in place. The AICPA has issued two sets of proposed criteria that will assist management **in designing and describing its cybersecurity risk management program, paving the way for independent, third-party attestation engagements by public accounting firms. These criteria provide a way for businesses to demonstrate due care and build confidence in their efforts.**

ControlCase
Compliance as a Service

Why SOC reports



User entities

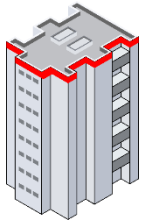


Service entities

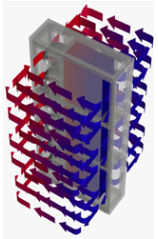
- Many entities function more efficiently and profitably by ***outsourcing tasks or entire functions*** to other organizations that have personnel, expertise, equipment, or technology to accomplish this tasks and functions.
- **User Entities** are responsible for assessing and addressing risks faced by the user entity related to **financial reporting**, including compliance with **laws and regulations** and the **efficiency and effectiveness of its operations.**
- The ownership and responsibility for the product or service provided to customers of the user entity cannot be delegated by User entities
- Management of the user entity is held responsible by those charged with governance, customers, shareholders, regulators, and other affected parties for establishing effective internal control over outsourced functions.

ControlCase
Compliance as a Service

Why SOC reports



User entities



Service entities

Obtaining Evidence of the Operating Effectiveness of Controls at a Service Organization

a) **Obtaining and reading a type 2 report, if available**
b) Performing appropriate tests of controls at the service organization by the user auditor.
c) Using another auditor to perform tests of controls at the service organization on behalf of the user auditor

ControlCase
Compliance as a Service

SOC ENGAGEMENTS

SOC 1sm	SOC 2sm	SOC 3sm
Controls at a service organization relevant **to user entities internal control over financial reporting.**	Controls at a service organization relevant **to security, availability, processing integrity confidentiality, or privacy.** Emphasizing in technology related service organizations.	Controls at a service organization relevant **to security, availability, processing integrity confidentiality, or privacy.**
Use of the SOC 1sm report is generally restricted to user entities and their auditors.	Use of the SOC 2sm report is generally restricted.	Use of the SOC 3sm report is generally restricted.
AICPA Guide, Applying SSAE No. 16, Reporting on Controls at a Service Organization	AT 101, Attestation Engagements of SSAEs using the predefined criteria in **Trust Services Principles**, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy.	AT 101, Attestation Engagements AICPA Technical Practice Aid, Trust Services Principles, Criteria, and Illustrations
Purpose: Reports on controls for F/S Audits	Purpose : Reports on controls related to compliance or operations	

ControlCase
Compliance as a Service

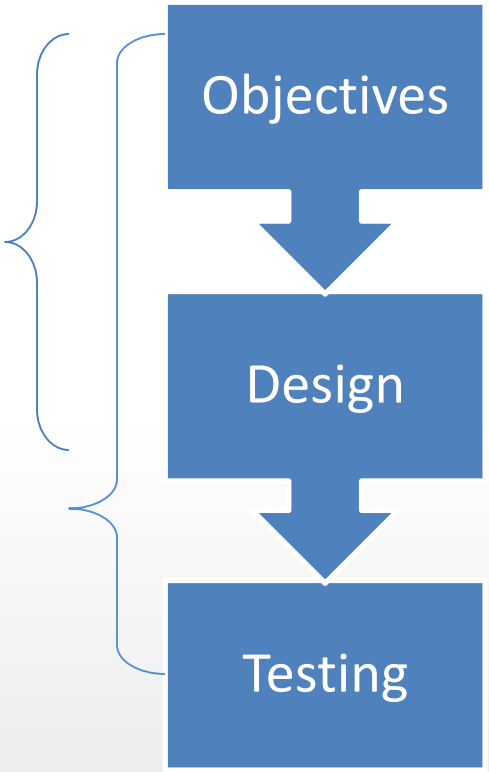
SOC TYPES

Type 1

- A report on management's description of the service organization's system and the suitability of the design of the controls.

Type 2

- A report on management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls.



ControlCase
Compliance as a Service

WHEN ARE THEY APPLICABLE?

TYPE 1 when….

- The service organization has not been in operation for a sufficient length of time to enable the service auditor to gather sufficient appropriate evidence regarding the operating effectiveness of controls.
- The service organization has recently made significant changes to the system and related controls and does not have a sufficient history with a stable system to enable a type 2 engagement to be performed.

TYPE 2 when….

- Standard assessment report required by user entities to comply with SOX section 404.

ControlCase
Compliance as a Service

SOC 2 – AT 101

ControlCase
Compliance as a Service

SERVICE RESOURCES

INFRASTRUCTURE

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

SOFTWARE

- The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).

DATA

- Transaction streams, files, databases, tables, and output used or processed by a system.

PROCESS

- The automated and manual procedures.

PEOPLE

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

ControlCase
Compliance as a Service

SOC 2 - OBJECTIVES

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 the AICPA and CICA.

ControlCase
Compliance as a Service

SOC 2 - TRUST SERVICES PRINCIPLES

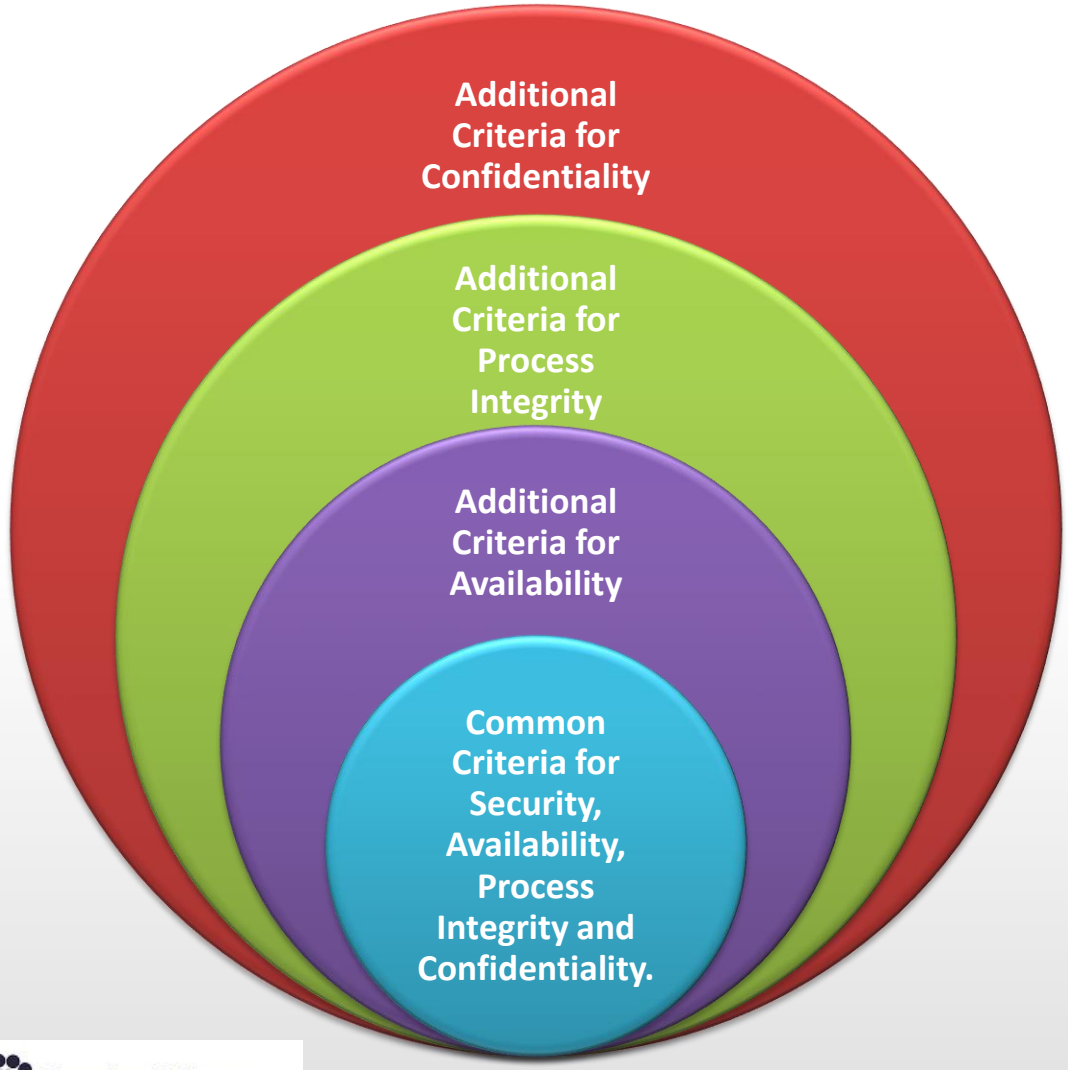
The ASEC Trust Information Integrity Task Force is focused on updating and maintaining the Trust Services Principles and Criteria (TSPC) and creating a framework of principles and criteria to provide assurance on the integrity of information.

Trust Services are a set of professional attestation and advisory services based on a core set of principles and criteria that address the risks and opportunities of IT-enabled systems and privacy programs.

The TSPC of security, availability and processing integrity are used to evaluate whether a system is reliable. The TSPC can be found in the publication *Trust Services Principles, Criteria and Illustrations*.

ControlCase
Compliance as a Service

Trust Services Principles



General Accepted Privacy Principles

ControlCase
Compliance as a Service

Common and additional Criteria

Common Criteria

- CC1 Organization and Management
- CC2 Communications
- CC3 Risk Management and Design and Implementation of Controls
- CC4 Monitoring of Controls
- CC5 Logical and Physical Access Controls
- CC6 System Operations
- CC7 Change Management

Additional Criteria

- Availability
- Processing Integrity
- Confidentiality

ControlCase
Compliance as a Service

SOC 1 – SSAE 16 / AT 801

ControlCase
Compliance as a Service

The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

COSO PRINCIPLES		
	OPERATIONS **FINANCIAL REPORTING** **COMPLIANCE**	**AREAS OF INTEREST**
Control Environment	Demonstrates commitment to integrity and ethical values	Policies, procedures
	Exercises oversight responsibility	Policies, procedures approval and annual update
	Establishes structure, authority, and responsibility	Org Chart, Job descriptions, Policies and procedures
	Demonstrates commitment to competence	Employee Handbook, HR Policies
	Enforces accountability	HR policies
Risk Assessment Process	Specifies suitable objectives Identifies and analyzes risk Assesses fraud risk Identifies and analyzes significant change	Risk assessment process: Identification, Assessment, Response, Reporting
Control Activities	Selects and develops control activities Selects and develops general controls over technology Deploys through policies and procedures	IT controls, access controls, firewal reviews, AV configuration, logging and monitoring activities. IDS/IPS
Information and Communication	Uses relevant information	Description of the system
	Communicates internally	Training records, HR policies, employees aknowledging policies and procedures
	Communicates externally	Vendors and Customers
Monitoring	Conducts ongoing and/or separate evaluations	Management/Operations meetings, IT audit, AV audit, IC efectiveness evaluation
	Evaluates and communicates deficiencies	Policies, procedures to communicate client complaints, systems failure.

ControlCase
Compliance as a Service

Management Assertions - Transactions

	Service Entity*	User Entity
OCCURRENCE The transactions actually took place.	X	X
COMPLETENESS All transactions that should have been recorded are recorded.	X	X
ACCURACY The transactions were recorded at the appropriate amounts.	X	X
AUTHORIZATION All transactions were properly authorized.	X	X
CUTOFF The transactions have been recorded in the correct accounting period.	X	X
CLASSIFICATION The transactions have been recorded in the proper accounts.	X	X

ControlCase
Compliance as a Service

Mgmt. Assertions – Accounts Balance

	Service Entity*	User Entity
EXISTENCE: Assets, liabilities and equity balances exist.	x	x
RIGHTS AND OBLIGATIONS: The entity holds or controls the rights to its assets and owes obligations to its liabilities.	x	x
COMPLETENESS: All assets, liabilities and equity balances that should have been recorded have been recorded.	x	x
VALUATION AND ALLOCATION: Assets, liabilities and equity balances are included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded.		x

ControlCase
Compliance as a Service

Mgmt. Assertions – Presentation and Disclosure

	Service Entity*	User Entity
OCCURRENCE: The transactions have occurred.		x
RIGHTS AND OBLIGATIONS: The transactions pertained to the entity.		x
COMPLETENESS: All disclosures that should have been included in the Financial Statements have been included.		x
CLASSIFICATION AND UNDERSTANDABILITY: Financial Statements are appropriately presented and described, and information in disclosures is clearly expressed.		x
ACCURACY AND VALUATION: Financial and other information is disclosed fairly and at appropriate amounts.		x

ControlCase
Compliance as a Service

Thank You !

ControlCase
Compliance as a Service