New standards and options

Service Org Report I (SOC I)

SSAE 16 – Service auditor guidance

Restricted use report (Type I or II)

Purpose – Reports on controls for F/S audits

Historically SAS70 reports

Service Org Control 2 (SOC 2)

AT 101

Generally restricted use report (Type I or II)

Purpose: Reports on controls related to compliance or operations

Truest service principles & criteria

Service Org Control 3 (SOC 3)

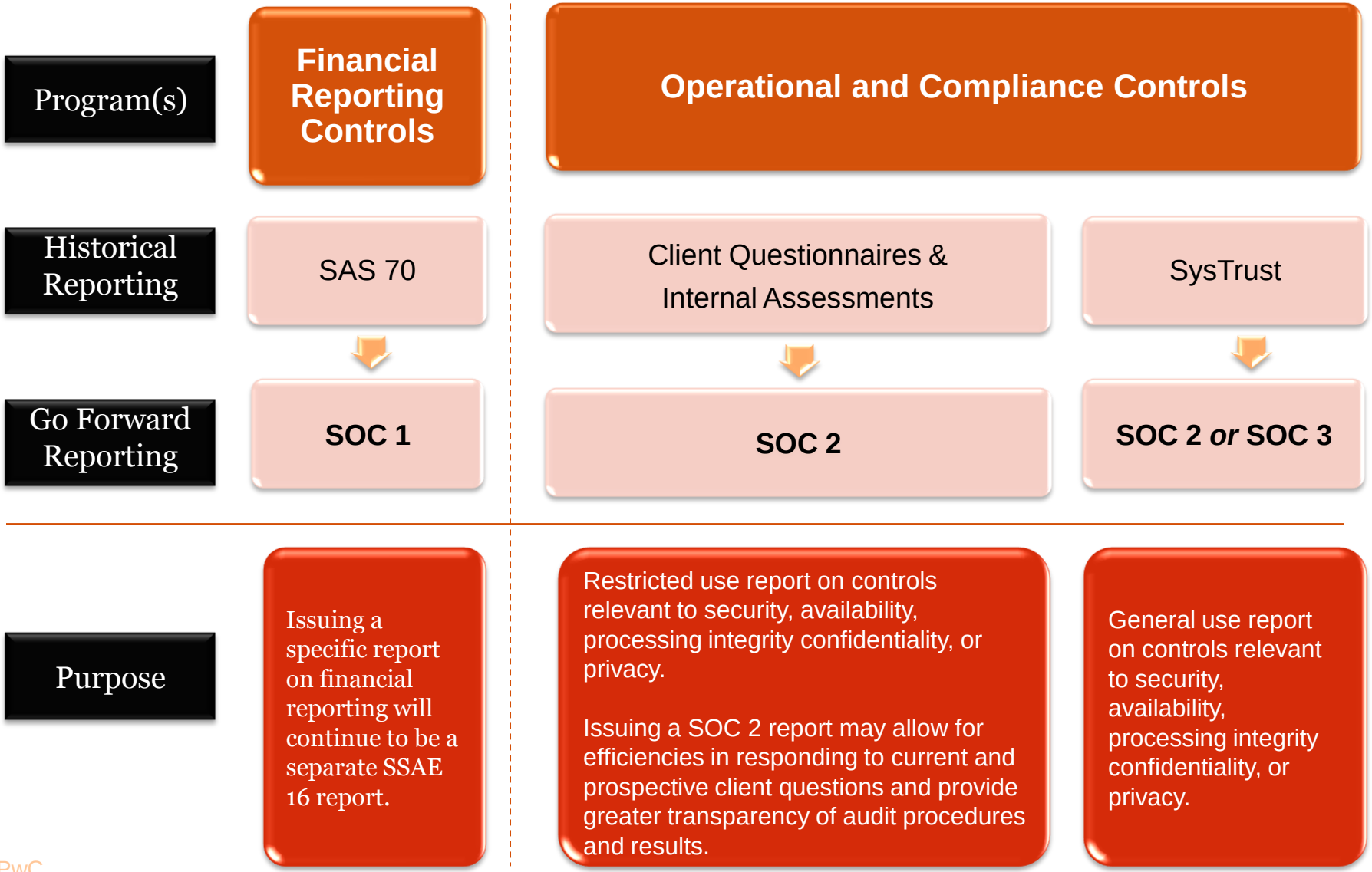
AT 101

General use report (w/ public seal)

Purpose – Reports on controls related to compliance or operations

Truest service principles & criteria

SOC Reporting Summary



Subject Matter

SOC 2 reports are for engagements that report on controls at a service organization that are intended to mitigate risks related to the Trust Service Principles. The Trust Service Principles are:

AICPA Trust Principle	Description
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 disposed of or anonymized in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles (GAPP)

Subject Matter - Sections

Each of the Trust Service Principles are divided into the following sections:

Section	Description
Policies	The entity has defined and documented its policies relevant to the particular principle.
Communications	The entity has communicated its defined policies to authorized users.
Procedures	The entity uses procedures to achieve its objectives in accordance with its defined policies.
Monitoring	The entity monitors the system and takes action to maintain compliance with its defined policies.

A SOC 2 can be performed on any one, or multiple principles. However, the entire principle(s) (all sections) must be assessed.

Components of a SOC 2 report

Report Section	Comparison to legacy SAS70 Reports
Executive Summary	Did not exist in legacy SAS70 reports
Section I: Independent Service Auditor's report (Opinion)	Opinion will be similar in layout/content to legacy SAS70
Section II: Management Assertion	Did not exist in legacy SAS70 reports
Section III: System Description Overview (provided by the service organization)	Similar in layout/content to legacy SAS70 but focused on the applicable trust principles/regulations
Section IV: Topical Area System Description (provided by the service organization), Testing and Results (provided by the service auditor)	Topical areas are new. The testing matrix will be similar to legacy SAS70.
Section V: Other Information Provided by the Service Organization	Similar in layout/content to legacy SAS70

SOC 3 - Overview

SOC 3 is SysTrust for Service Organizations

- Use
  - Distribute the SOC 3 report to customers and publicly display a seal of approval using the SOC report: SysTrust for Service Organization seal.
- Scope
  - SOC3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality, and privacy)
- www.webtrust.org