PANEL ON SOC 2 AND SOC 2+ ASSURANCE SERVICES
# FRI, 2/7/2025: 11:00 AM - 12:30 PM EST

ROOM: SCHMIDT FAMILY COMPLEX 112, FLORIDA ATLANTIC UNIVERSITY

Moderator: Efrim Boritz, Professor And CPAO Chair, University of Waterloo

Panelists

- **Nancy Bagranoff, Professor, Richmond University**

- **Chris Halterman, EY (Retired Chair Of AICPA Trust Services Working Group)**

- **Sean Linton, Partner, Eisner Advisory Group LLC, Chair Of AICPA Trust Services Working Group**
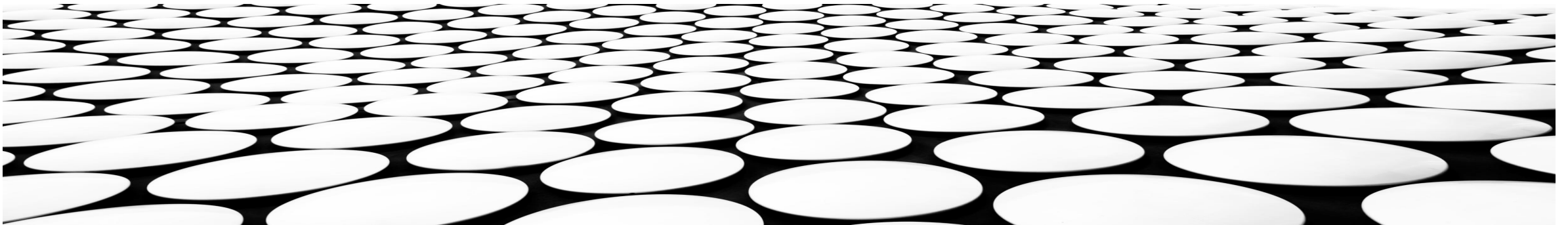
Nancy Bagranoff, DBA, CPA

is University Professor (Accounting) at the University of Richmond. Professor Bagranoff was Dean of the Robins School from 2010 until 2019. Prior to that appointment she served as Professor of Accounting and Dean of the College of Business and Public Administration at Old Dominion University. Dr. Bagranoff has taught at several universities, including American University, George Mason University, and Miami University. Her areas of teaching and research are accounting, accounting information systems, and cybersecurity. In addition to publishing many research articles, she has co-authored books on the topics of accounting information systems, information systems auditing, accounting education, and consulting. In 2021, she received the AICPA Distinguished Achievement in Accounting Education award. She has been President of the American Accounting Association and Chair of the Greater Richmond Chamber of Commerce. She served on the Board of Directors of the AICPA and the Association to Advance Collegiate Schools of Business (AACSB).

Chris Halterman, CPA

has more than 36 years of experience in the public accounting profession, focusing on internal control reporting, IT audit and information integrity. Prior to his retirement in June 2024, he led E&Y's Advisory System and Organization Control Reporting practice globally and in the Americas, with responsibility for developing methodology, training, client service strategy, quality assurance programs and market initiatives. Chris is a member of several AICPA working groups related to SOC reporting and was formerly a member of the AICPA Assurance Services Executive Committee (ASEC). He chaired the ASEC Trust/Information Integrity Task Force from 2008 to 2024. In this role, he led the development of the AICPA SOC for Cybersecurity, SOC 2, data integrity reporting frameworks, including revisions to the trust services criteria for evaluating the system security, availability, processing integrity, confidentiality and privacy. In his role, Chris speaks on cybersecurity reporting, and SOC 1 and SOC 2 reporting.Chris graduated from the University of Wisconsin-Madison-Masters of Accountancy (Accounting and Auditing); University of Iowa-Bachelor of Science (Mathematics and Economics)

Sean Linton, CPA, CITP

is an Audit Partner at EisnerAmper providing assurance and technology control services. He specializes in System and Organization Controls (SOC) examinations, risk assessments, and information systems advising and strategy, and has deep expertise in multiple audit disciplines. Sean has served organizations from across the business spectrum, from small investment firms to large international corporations. As a SOC auditor, he helps his clients devise and execute audit strategies to meet myriad compliance and regulatory requirements related to data security and system integrity. Over the years, Sean has led international audits in the UK, France, Hong Kong, India, and Taiwan, with much of that fieldwork being performed abroad. These experiences have allowed him to become well versed in international reporting and compliance frameworks, in addition to his detailed knowledge of U.S. reporting guidance and regulations. Prior to joining EisnerAmper, Sean was an Audit Partner providing technology and consulting services at Lurie LLP, a Minneapolis-based accounting and advisory firm, which provided clients with solutions in accounting, audit, tax planning and wealth management, serving business leaders in a wide variety of industries including health care, professional services, technology, manufacturing, real estate and more. As an active member of the American Institute of Certified Public Accountants (AICPA), Sean serves as the current chair of the AICPA's SOC 2 task force and is also a national instructor teaching SOC-focused courses to CPAs around the country. Sean is also a peer reviewer and performs enhanced oversight reviews of SOC engagements for the AICPA's peer review program. He lives in Dallas, Texas with his wife and 4 children.

Dr. J. Efrim Boritz, FCPA, CISA

is the Ontario CPAs' Chair in Accounting in the School of Accounting & Finance at the University of Waterloo, Canada. He is also the founding Director of the [University of Waterloo Centre for Information Integrity and Information Systems Assurance](#).
Dr. Boritz is the author or co-author of numerous books, monographs, book chapters and articles in academic and professional journals and has served on numerous editorial boards. His research focuses on professional practice in external and internal auditing, particularly in the context of information systems, with the goal of enhancing professional judgment through better quality information, models and processes.

Dr. Boritz has served on numerous task forces and committees of domestic and international professional and academic associations. He is a former president of the Canadian Academic Accounting Association which has given him all three of its major teaching, research and service awards. The Council of the Institute of Chartered Accountants of Ontario gave him its highest award, the Award of Outstanding Merit in 1999. In 2010 he received the Canadian Institute of Chartered Accountant's Bill Swirsky Innovation Leadership Award and in 2012 he received the Queen Elizabeth II Diamond Jubilee Medal. In 2023 he was inducted into the Canadian Accounting Hall of Fame and in 2025 he has been awarded ISACA's Global Excellence in Education award. He is a member of the AICPA's Information Integrity, Trust Services and Cybersecurity Working Groups.
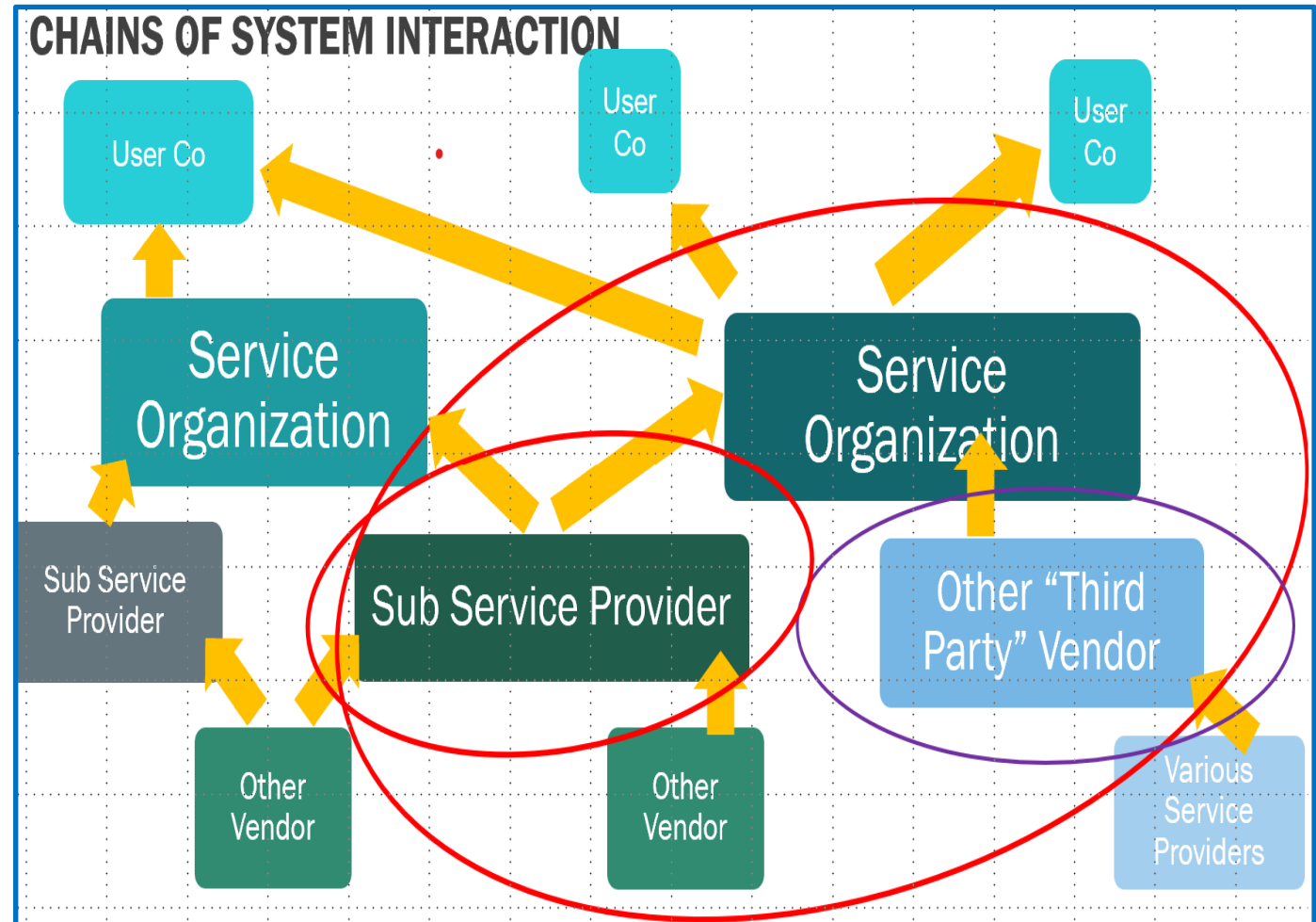
PANEL ON SOC 2 AND SOC 2+ ASSURANCE SERVICES

Panelists will address:

- the nature of SOC 2® services, the demand for those services and suppliers of those services, including distinction between SOC 1 and SOC 2

- variations of SOC 2® services that address criteria other than TSC and the risks they raise for providers and users of SOC 2® and SOC 2+ reports, and non-CPA firm competitors in the market for assurance on system and organization controls

- key elements of SOC 2® reports and how SOC 2® reports should be used

- service quality monitoring and other quality assurance initiatives

- competency requirements for CPAs and non-CPA providers of SOC 2® related services

- research opportunities

- how future developments may affect SOC 2® services.

Why was SOC 2 originally developed?

- **Growth in outsourcing and cloud computing**

- **Demands for assurance on reliability of outsourced systems**

- Service organizations were using standards designed for internal control over financial reporting to issue assurance reports **which did not cover broader system reliability objectives**

- It was essential to **separate** controls over financial reporting from other control objectives

CHAINS OF SYSTEM INTERACTION

User Co · User Co · User Co · Service Organization · Service Organization · Sub Service Provider · Sub Service Provider · Other "Third Party" Vendor · Other Vendor · Other Vendor · Various Service Providers
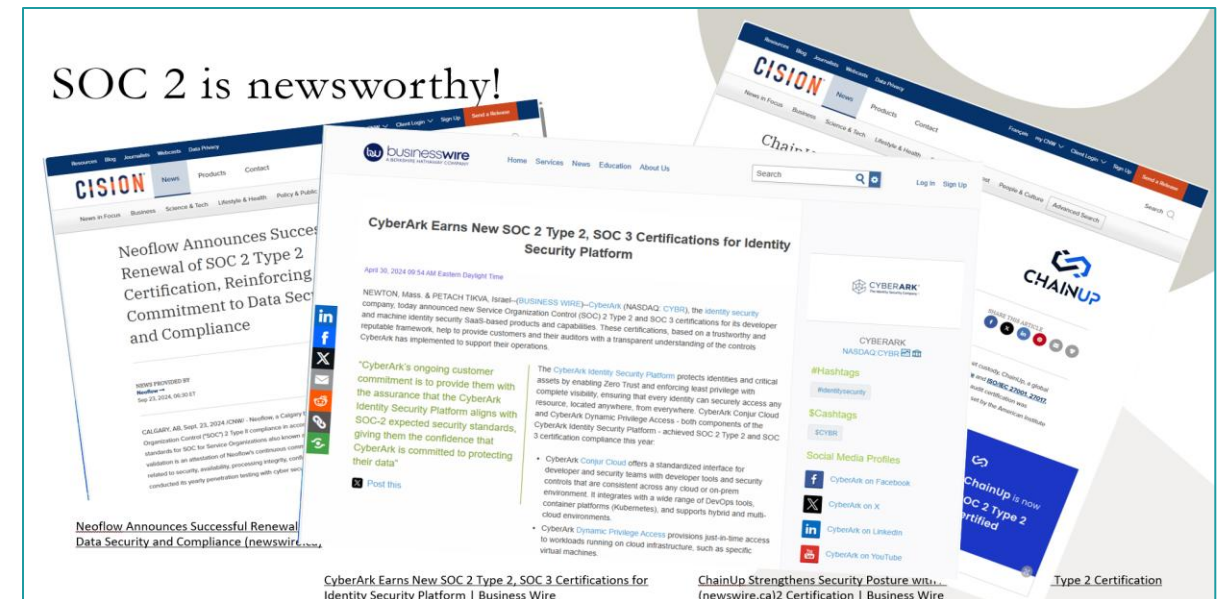
WHY AN ASSURANCE REPORT?

- **Confidence in Business Partners' Systems**
  - common evaluation framework - baseline
  - better selection of business partners

- **Confidence in Internal Systems**
  - appropriate controls
  - protect shareholder value
  - better decision making

- **Reduce Costs**
  - avoid systems development rework
  - avoid reputation / market-share / other losses
  - avoid disruption from having customers onsite seeking to obtain comfort about system reliability
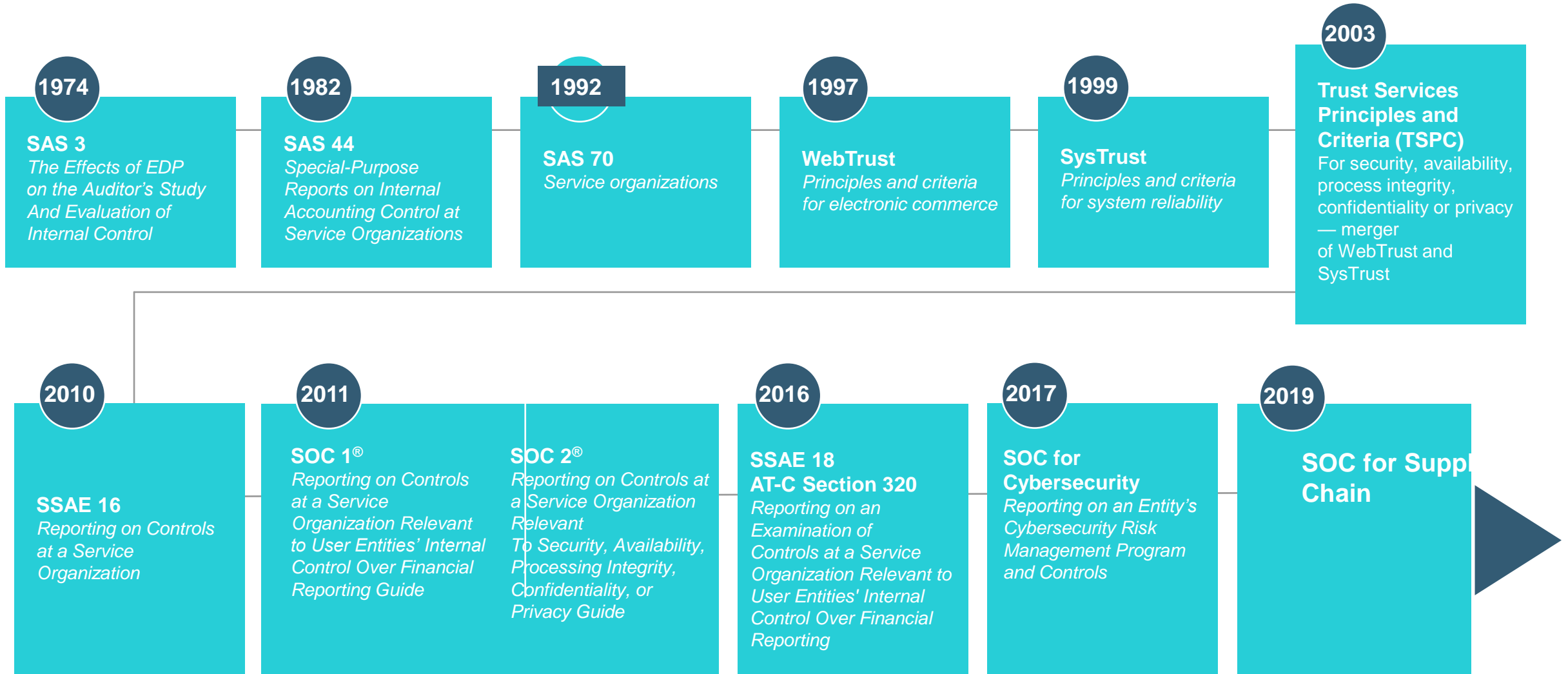
Other Stakeholder needs
- Regulators (taxation, banking, markets, etc...)
- Insurers

Marketing of System-based Services
- differentiate against competitors

SOC 2 and SOC 2+

EVOLUTION OF SOC TO THE PRESENT DAY

1974

SAS 3
The Effects of EDP on the Auditor's Study And Evaluation of Internal Control

1982

SAS 44
Special-Purpose Reports on Internal Accounting Control at Service Organizations

1992

SAS 70
Service organizations

1997

WebTrust
Principles and criteria for electronic commerce

1999

SysTrust
Principles and criteria for system reliability

2003

Trust Services Principles and Criteria (TSPC)
For security, availability, process integrity, confidentiality or privacy — merger of WebTrust and SysTrust

2010

SSAE 16
Reporting on Controls at a Service Organization

2011

SOC 1®
Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide

SOC 2®
Reporting on Controls at a Service Organization Relevant To Security, Availability, Processing Integrity, Confidentiality, or Privacy Guide

2016

SSAE 18 AT-C Section 320
Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting

2017

SOC for Cybersecurity
Reporting on an Entity's Cybersecurity Risk Management Program and Controls

2019

SOC for Supply Chain

SOC 2 and SOC 2+

STANDARDS GOVERNING SOC SERVICES

Service	US	CDA	International
General References	SSAE 18	CSAE 3000	ISAE 3000
SOC 1 (Financial Reporting) • User Entity Auditor • Service Auditor	AU 324/AS 2601 SSAE 18	CAS 402 CSAE 3416	ISA 3402 ISAE 3402
SOC 2, 3 System Commitments & Requirements System reliability Security, Availability, Processing Integrity, Confidentiality, Privacy	SSAE 18 • Description Criteria • Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, Privacy	CSAE 3000/3001	ISAE 3000/3001
SOC 2 + (System reliability based on Trust Services Criteria **and Additional Criteria**)	SSAE 18 Third Party Assessment Engagements (Q&A 9550)	CSAE 3000/3001	ISAE 3000/3001
Professional Codes of Conduct/Quality Control	AICPA Professional Standards, Statements on Quality Management Standards (SQMS 1, SQMS 2)	Canadian Standards on Quality Management (CSQM1, CSQM2)	International Standards on Quality Management (ISQM1, ISQM2)

DEMAND FOR SOC SERVICES

- Differences between SOC 1 and SOC 2 services?

- Who are the users of these services?

SOC 1 AND SOC 2 REPORTS

- Both are for service organizations, their users and their auditors, though the type and nature varies

- Both have Type 1 and Type 2 reports

- Both require a CPA

- Both are governed by SSAE 18 standards and guidance for attestation engagements (ISAE 3000 internationally)

SOC 1 REPORTS

- Internal controls over user financial statements (ICFR)

- For service organizations providing services impacting financial reporting (e.g., payroll processors, accountants, or any company handling financial data)

- Allows management to fulfill regulatory responsibilities for ICFR

- Recipients are user entities and their auditors (for risk assessments and audit evidence)

- Use is restricted to User Entity

SOC 2 REPORTS

- Internal controls over data security plus one or more of: availability, processing integrity, confidentiality, privacy

- For third parties providing services maintaining or processing data

- Generally broader in scope than SOC 1 reports

- Provides some cybersecurity assurance for affiliates of service organizations

- Use is restricted to User Entity

SOC 3 REPORTS

- SOC 3 is similar to SOC 2
but while SOC 2 is restricted to use by the user entity, the
SOC 3 is for general use and may be used as marketing material

MANAGEMENT ASSERTIONS

SOC 1:

Management description fairly presents the service organization's system

Assertion that controls related to management's described control objectives are suitably designed (Type 1) and operated effectively (Type 2) to achieve control objectives.

SOC 2:

Management description is in accordance with Description Criteria

Assertion that controls are suitably designed (Type 1) and operated effectively (Type 2) to provide reasonable assurance that **service commitments and system requirements** were achieved based on applicable Trust Services Criteria.

AUDITOR'S ASSERTIONS

SOC 1:

Opinion on management's assertion that their description is a fair representation

Opinion on assertion that controls were suitably designed (Type 1) and operated effectively (Type 2) to achieve control objectives.

Description of auditor tests of controls and results

SOC 2:

- Opinion whether management description is in accordance with Description Criteria

- Opinion that controls in the system were suitably designed (Type 1) and operated effectively (Type 2) to provide reasonable assurance that service commitments and system requreiemnts were achieved based on applicable Trust Services Criteria.

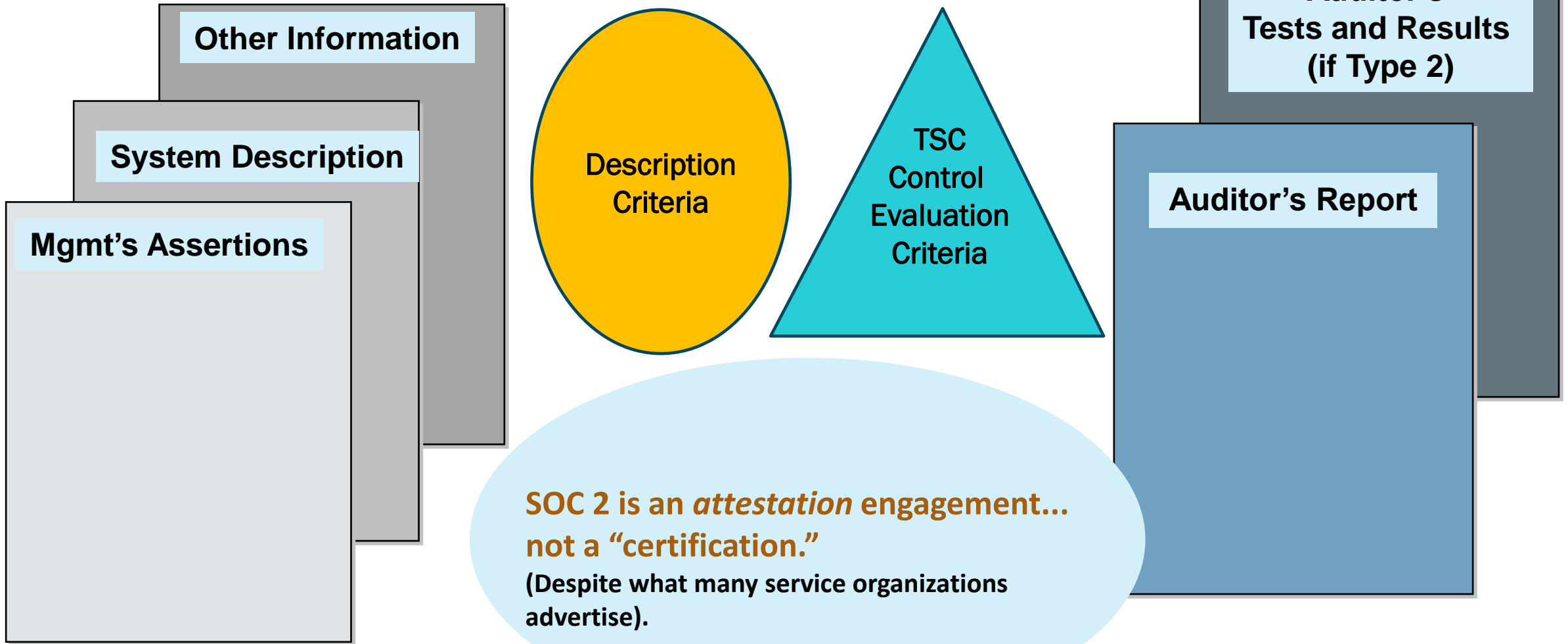- Description of auditor tests of controls and results
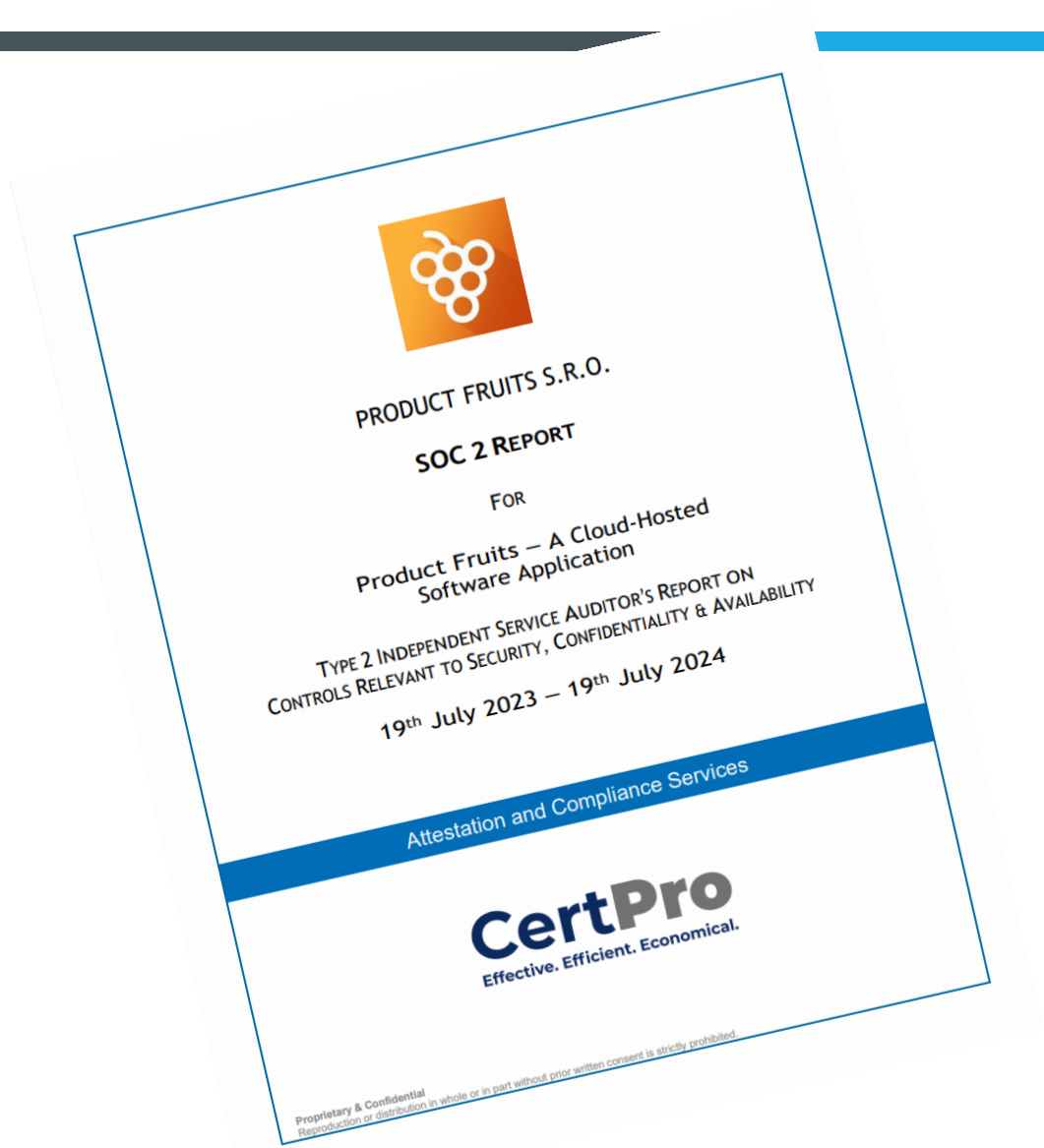
SUPPLIERS OF SOC SERVICES

- Who are the suppliers of SOC services?

- What issues have been observed around the provision of these services?

KEY ELEMENTS OF SOC 2® REPORTS

- Key elements of SOC 2® reports

COMPONENTS OF SOC 2

Other Information

System Description

Mgmt's Assertions

Description Criteria

TSC Control Evaluation Criteria

Auditor's Tests and Results (if Type 2)

Auditor's Report

SOC 2 is an *attestation* engagement... not a "certification."
(Despite what many service organizations advertise).

KEY ELEMENTS OF SOC 2® REPORTS

- How should SOC 2® reports be used?

COMPETITION

- Variations of SOC 2® services that address criteria other than TSC (that some have labeled as SOC2+ services).

- Competitors in the market for assurance on system and organization controls

- Issues they raise for providers and users of SOC 2® and SOC 2+ reports.

QUALITY CONTROL

- Processes in place for SOC service quality monitoring

COMPETENCIES

- Competency requirements for CPAs and non-CPA providers of SOC 2® related services

- Courses and materials to address these competencies

COMPETENCIES

- ONLY CPAs can prepare SOC 2 reports
- Preparation versus Use
- CPA ISC coverage:
      ISC Area III – Considerations for System and Organization Controls (SOC Engagements (15-25%)
- Knowledge of controls over TSC:
    - Confidentiality
    - Integrity
    - Availability
    - Security
    - Privacy
- General cybersecurity knowledge, IT infrastructure, risk assessment, risk management, cyber frameworks, relevant cyber laws and regulations

TEACHING SOC REPORTS

- SOC 1 typically covered in Auditing courses

- SOC 2 may be covered in AIS, IT Audit, or Cybersecurity courses

- Students need familiarity with Trust Services Criteria

- Cases can enhance learning about SOC reports

AICPA ASSURANCE REPORTING TODAY

- Uses the AICPA Attestation Standards (IAASB Assurance and AUP Standards)
- Focus on reporting on useful information
  - Provided by the responsible party
  - Provided by the practitioner
  - The challenge is to determine what is "useful information" in a particular set of circumstances
- Generally Applicable Criteria
  - Controls reporting based on the Trust Services Criteria (an augmentation of the COSO Internal Controls Framework) e.g., SOC 2, SOC 3, SOC for Cybersecurity, SOC for Supply Chain
  - Information reporting based on the AICPA Data Integrity Criteria
- Special purpose criteria (e.g., SOC 1)

FUTURE

- How will future developments affect SOC 2® services?

- What emerging trends will affect the demand and supply for SOC services?

- What is the future for SOC for Cybersecurity, SOC for Supply Chains and SOC for AI?

RESEARCH OPPORTUNITIES

- Published Research to Date:
  - Rarely academic research
  - No published accounting education papers
  - Practitioner journal research primarily opinion-based

- Opportunities:
  - SAS 2 quality ("fake reports")
  - Case Studies
  - SOC 2 usage versus other (survey paper – e.g., Makhija 2022)
  - How users verify SOC 2 quality
  - SOC 2 report motivation (versus other compliance)
  - Cybersecurity incidents where SOC 2 report exists - cause

Q&A

DOWNLOAD SLIDES FROM:

[PANEL ON SOC 2 AND SOC 2+ ASSURANCE SERVICES - FEB 2025 | UNIVERSITY OF WATERLOO CENTRE FOR INFORMATION INTEGRITY AND INFORMATION SYSTEMS ASSURANCE | UNIVERSITY OF WATERLOO](#)