Making sense of SOC 1, 2 & 3 in a world of competing control frameworks

(e.g., ISO 27001, NIST 800-53, etc.)

or, *forget about running out of oil, I'm worried about the world running out of acronyms*

Chris Halterman, Executive Director—Ernst & Young

Track Name - Session #

Agenda

- Setting the stage—the terms and players
- Vendor management of service organizations
- SOC 1,2,3
- Future direction
- Actions

SETTING THE STAGE—THE TERMS AND PLAYERS

Some of the control framework players

Organization	Framework	Coverage
NIST	800-53	security and availability
ISO	27001/27002	security and availability
CSA	CCM	security and availability
CMS	HIPAA	security and privacy
PCI Security Council	DSS	security
HITRUST	CSF	security and privacy

More to come

Relationship of Trust Services, SysTrust, WebTrust, and SOC 2

- **SOC 1 Report**—a report consisting of an unaudited management assertion, service auditor's report, and an audited system description of control relevant to user entities' internal control over financial reporting. A Type 2 report includes the auditor's tests of those controls
- **SOC 2 Report**—a report consisting of an unaudited management assertion, service auditor's report, and an audited system description of control relevant security, availability, processing integrity confidentiality and privacy based on the Trust Services Criteria. A Type 2 report includes the auditor's tests of those controls
- **SOC 3 SysTrust for Service Organizations (SOC 3)**—a SysTrust Report for a service organization's system that uses the SOC 3 seal rather than the SysTrust seal
- **Trust Services principles and criteria—**a set of suitable criteria used to evaluate internal control of a System as it relates to security, availability, processing integrity, confidentiality and privacy
- **Trust Services Report**—a general use examination report on a system prepared using AT101 Assurance Reporting consisting of an accountants report, management assertion and a short (approx. 4 pages), unaudited description
- **SysTrust Report**—a Trust Services Report complying with the SysTrust/WebTrust requirements for which a SysTrust seal has been issued and placed on the organization's website
- **WebTrust Report**—a Trust Services that includes the independent accountants' opinion on the organization's compliance with its commitments as they relate to security, availability, processing integrity, confidentiality and privacy and complies with the SysTrust/WebTrust requirements for which a WebTrust seal has been issued and placed on the organization's website

VENDOR MANAGEMENT
—OF SERVICE ORGANIZATIONS
—WITH MY BUDGET?
—SERIOUSLY?

CUSTOMER CHALLENGES

Internal control responsibilities—COSO

- Establish and maintain a system of internal control
  - Internal control should help achieve business objectives
    - Agility—adapting to changing business and operating environments
    - Confidence—mitigating risks to an acceptable level
    - Clarity—providing reliable information supporting sound decision-making
  - Internal control objectives
    - Effectiveness and efficiency of operations
    - Reliability of reporting
    - Compliance with applicable laws and regulations

An organization’s responsibility to maintain a system of internal control and managements accountability for that system of internal control do not change, if it uses a vendor to perform some business functions

Vendor risk management challenges

- Need to evaluate vendor risks and develop a risk treatment plan
- Strategy
  - Implement controls over vendors
  - Require vendors to implement controls
- Challenges
  - Too many vendors
  - Too many risks
  - Picking an evaluation framework
    - Too many frameworks
    - Multiple requirements
  - Too little time
  - Not enough budget

Risks related to vendor implementation of controls

Contracting for the vendor to perform the controls introduces new risks:

- The vendor does not implement the necessary controls
- The controls are not suitably designed
- The controls do not operate effectively

Point of view

In addition to contracting for services from a well controlled system, customers need to contract for:

- Evidence regarding the suitability of the design of the controls
- Evidence as to their effective operation

SERVICE PROVIDER CHALLENGES

Point of view

In addition to providing services from a well controlled system, service providers need to provide and contract to provide:

- Evidence regarding the suitability of the design of the controls
- Evidence as to their effective operation

Service provider's problem

Providing customers with a well controlled system as well as evidence as to the suitability of design and operating effectiveness of controls is costly

- Cost of controls—a topic for another day
- Cost of supplying evidence
  - Internal cost of delivering information
  - Disruption of operations
  - Consumption of time of key individuals
  - Fees paid to third-party assurance providers

AND NOW ALPHABET SOUP

Control frameworks and assurance

Control framework

- ISO 27001/27002
- PCI DSS
- FedRAMP
- CSA CCM

Assurance

- ISO 27001 Certification
- QSA report
- 3PAO report
- Open Security framework--developing

The challenge to assurance

With any form of assurance users want:

- Transparency with regard to the design and operation of controls
- Transparency with regard to the basis of the 3rd party assessor's conclusion

SOC 1, 2, 3
—WHAT WERE YOU THINKING?

SAS 70 and SysTrust—some history

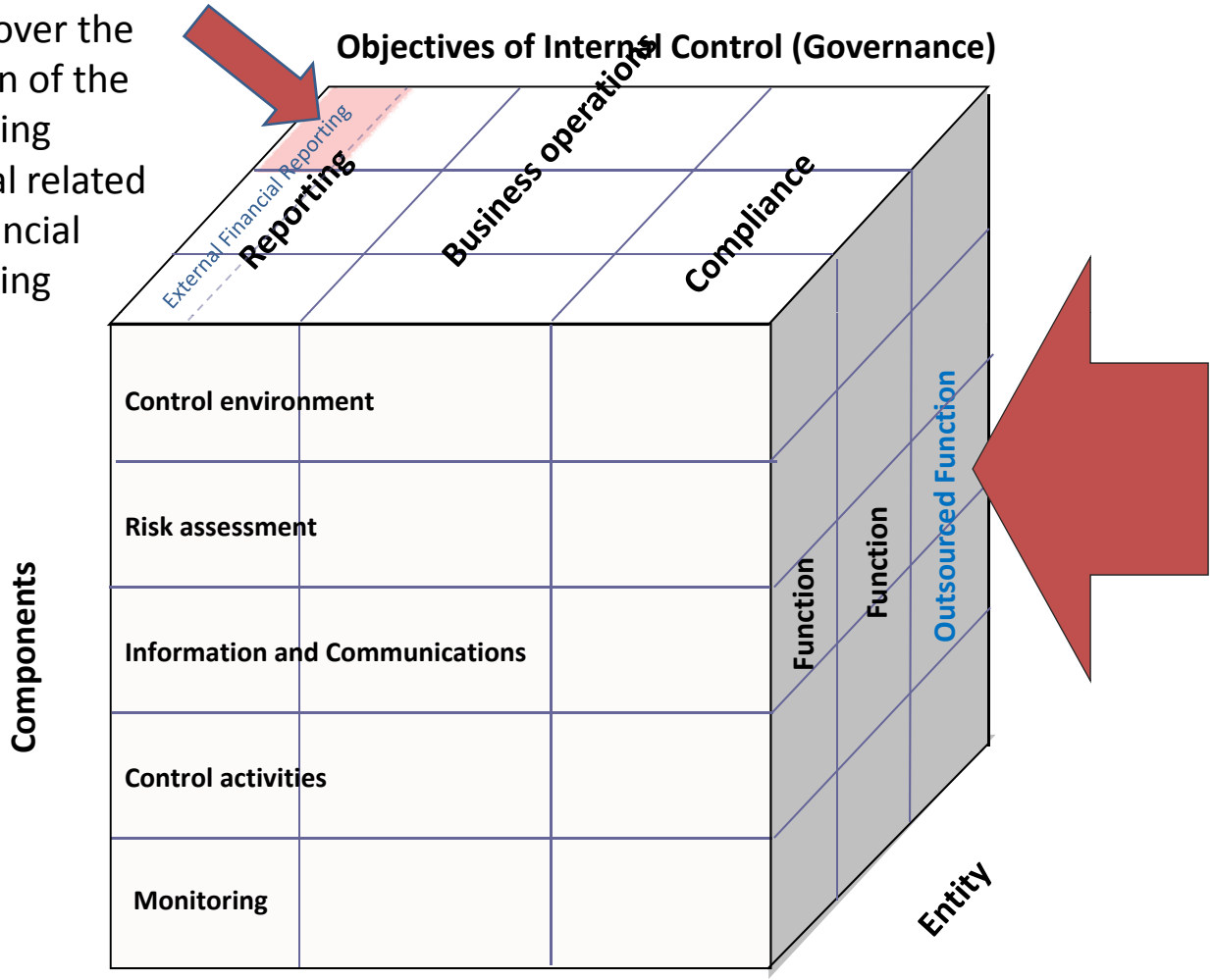
- SAS 70
  - Gained broad acceptance as a control reporting format
    - Design provided needed transparency
    - Scalability permitted use for both simple and complex systems
    - Critical for Sarbanes-Oxley
  - Limitations
    - Only addressed controls relevant to financial reporting
    - Stretching its intent caused a loss of reliability
    - Existing users only
- SysTrust
  - Public distribution
  - Addressed all aspects of systems
  - Provided no transparency

Increasing emphasis on internal control outside financial reporting

- Maturity of Sarbanes-Oxley programs
- Emphasis on Governance Risk and Control and Enterprise Risk Management
- Audit committee responsibility
- Growth in laws and regulations affecting companies
- Increased stakeholder expectations
- Regulatory concern
- Creation of compliance functions (e.g., Chief Compliance Officer)

Relationship of internal control to functions

SOC 1 reports only cover the portion of the reporting vertical related to financial reporting



Outsourcing moves an entity function to the service organization

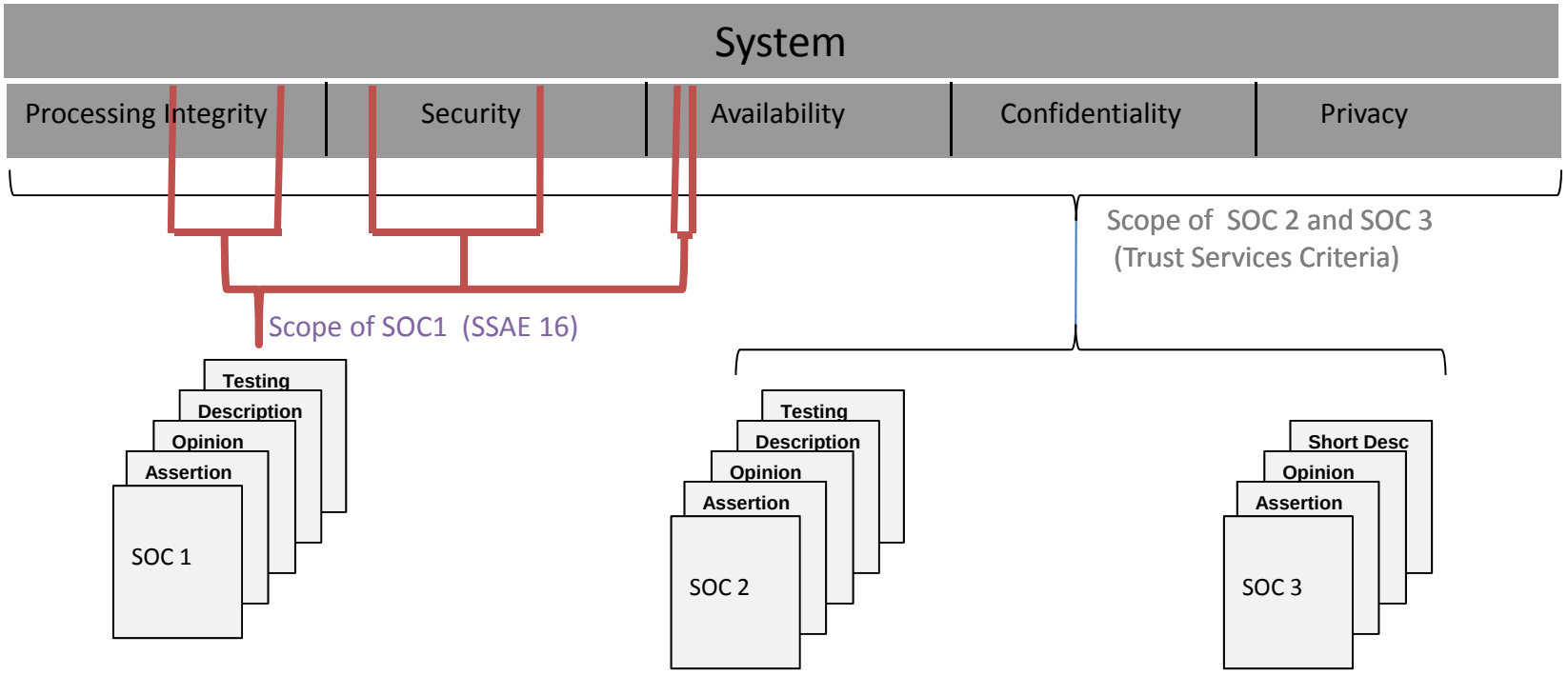
Development of SOC 1, 2 and 3

- SOC 1
  - Determined that it is only intended for financial reporting uses
  - Update of SAS 70
  - Need to establish a name that will not change when a new standard was issued
- SOC 2
  - A “SOC 1” for everything else
  - Problem with control objectives—solution Trust Services criteria
  - Need to be able to integrate with other control frameworks
  - There were no good acronyms
- SOC 3
  - Relating SysTrust to SOC 1 and SOC 2

Trust Services Principles

- 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 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 Canadian Institute of Chartered Accountants.

SOC 1, SOC 2, SOC 3 Comparison



Users:
- User entity controller
- User entity SOX department
- User auditor

Users:
- User entity security
- User entity compliance
- User entity vendor management
- Regulators
- Prospective user entities

Users:
- General public

Integration with various frameworks

Business concerns ⇨ Trust Services principles

Process objectives ⇨ Trust services criteria

Process controls ⇨ Suitable control framework

- ISO 27001/27002
- NIST 800-53
- HITRUST CSF
- HIPAA
- Others

SINCE WE'RE IN THIS TOGETHER, DO YOU MIND TELLING ME WHERE WE ARE HEADED?

Path ahead

- Working with various control framework sponsors
- Update the Trust Services criteria
- Additional guidance
  - AICPA
  - ISACA
  - CSA
  - Others?

Revisions to Trust Services criteria

- Principles stay the same
- Restructuring away from current grouping to a more process focus
- Additional emphasis on
  - Management processes
  - Risk assessment
  - Wording criteria for clarity
  - Update of availability

WHAT CAN WE DO?

How to help

Service providers

- Work in industry groups
- Don’t re-invent frameworks
- Develop a strategy
- Address evidence of design and operation of controls as a part of your service

Customers

- Work in industry groups
- Don’t re-invent frameworks
- Know what you need and negotiate for it
- Be flexible

QUESTIONS?

Thank you


ISACA
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA