System and Organization Control (SOC) for Cybersecurity

Answers for Jittery Management

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Create Opportunities

Disclaimers

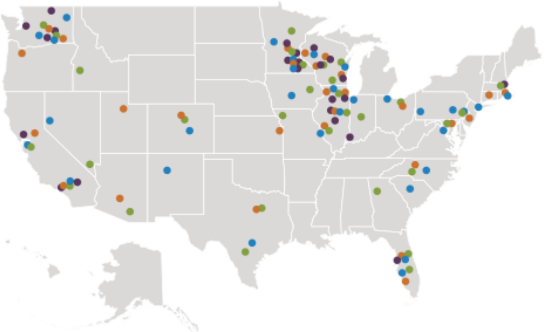
The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

Housekeeping

- If you are experiencing technical difficulties, please dial: 800-422-3623.
- Q&A session will be held at the end of the presentation.
  - Your questions can be submitted via the Questions Function at any time during the presentation.
- The PowerPoint presentation, as well as the webinar recording, will be sent to you within the next 10 business days.
- For future webinar invitations, subscribe at CLAconnect.com/subscribe.
- Please complete our online survey.

About CLA

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting



- More than 5,400 employees
- Offices coast to coast
- CLA's information security team combines certified technical professionals, including system administrators and network engineers, with CPAs who have key industry and IT audit experience.

Learning Objectives

- At the end of this session, you will be able to:
  - Identify factors driving the need for cybersecurity assurance reporting
  - Describe the differences between SOC reporting options
  - Explain the scope and criteria used as the basis for SOC for Cybersecurity reporting

Drivers for Cybersecurity Assurance

Cybersecurity Definition

cybersecurity

Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

National Initiative for Cybersecurity Careers and Studies
https://niccs.us-cert.gov/glossary#C

Cyber Fraud Themes

Hackers have "monetized" their activity

- More sophisticated hacking
- More "hands-on" effort
- Smaller organizations targeted
- Cybercrime as an industry

Everyone is a target…

Phishing is a root cause behind the majority of cyber fraud and hacking attacks

Largest Cyber Fraud Trends - Motivations

Black market economy to support cyber fraud

- Business models and specialization

Most common cyber fraud scenarios we see affecting our clients

- Theft of PII and PFI
- Theft of credit card information
- (Corporate) account take overs
- Ransomware and Interference

What is Driving the Need of Assurance

Increased risk of cyber threats

- **Increase of converging data (Big Data)**
  - Financial
  - Medical
  - Demographics
  - GPS
  - Internet history
  - Intellectual Property
- **Increasing frequency of events**

Real World Examples

City of Atlanta – Ransomware

Deloitte

Equifax

Cambridge Analytica

What is Driving the Need of Assurance

External Governance

- Banking Regulations >
  FFIEC Cybersecurity Assessment Tool
- Healthcare >
  CMS Information Security and Privacy
- Public Filings >
  Statement of Cybersecurity Interpretive Guidance
- Federal Government >
  NIST Cyber Security Framework

What is Driving the Need of Assurance

Board of Directors and other charged with governance

- Managing risk
- Managing insurance cost
- Managing compliance
- Managing public image

How SOC Provides Cybersecurity Assurance

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

History

SAS70: Early 1990’s	Internal Controls over service organizations
SSAE 16: April 2010	Established SOC1 and SOC2
SSAE 18: April 2016	Recodified SSAE 16
SOC for Cybersecurity: April 2017	

Different Reports

SOC1	Internal Controls over Financial Reporting
SOC2	Internal Controls over Security, Availability, Confidentiality, Processing Integrity, and/or Privacy
SOC for Cybersecurity	An examination engagement to report on whether (a) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (b) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

What are the differences

Factor	SOC 1	SOC 2	SOC 3	SOC for Cybersecurity
Internal Controls over Financial Reporting	X			
Internal Controls to Address Criteria		X	X	X
Internal Controls over Cybersecurity Program				X
Restricted Report	X	X		

Basis of the SOC for Cyber Security

Description Criteria to be including in the system description

- 19 criteria grouped in to 9 sub groups

Trust Service Criteria to be tested for operating effectiveness

- Security, Availability, and Confidentiality

Description Criteria

Cybersecurity Risk Management Program Criteria

NATURE OF BUSINESS AND OPERATIONS

DC1: The nature of the entity’s business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed

NATURE OF INFORMATION AT RISK

DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity

CYBERSECURITY RISK MANAGEMENT PROGRAM OBJECTIVES

DC3: The entity’s principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing

DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity’s objectives

Description Criteria

Cybersecurity Risk Management Program Criteria

FACTORS THAT HAVE A SIGNIFICANT EFFECT ON THE INHERENT CYBERSECURITY RISK

DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity, (2) organizational and user characteristics, and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and in its environment.

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of those incidents and their disposition

CYBERSECURITY RISK GOVERNANCE STRUCTURE

DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program

DC8: The process for board oversight of the entity's cybersecurity risk management program

DC9: Established cybersecurity accountability and reporting lines

DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities

Description Criteria

Cybersecurity Risk Management Program Criteria

CYBERSECURITY RISK ASSESSMENT PROCESS

DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners

CYBERSECURITY COMMUNICATIONS AND QUALITY OF CYBERSECURITY INFORMATION

DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program

Description Criteria

Cybersecurity Risk Management Program Criteria

MONITORING OF THE CYBERSECURITY RISK MANAGEMENT PROGRAM

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

CYBERSECURITY CONTROL PROCESSES

DC17: The process for developing a response to assessed risks, including the design and implementation of control processes

DC18: A summary of the entity's IT infrastructure and its network architectural characteristics

DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:

a. Prevention of intentional and unintentional security events

b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents

c. Management of processing capacity to provide for continued operations during security, operational, and environmental events

d. Detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability

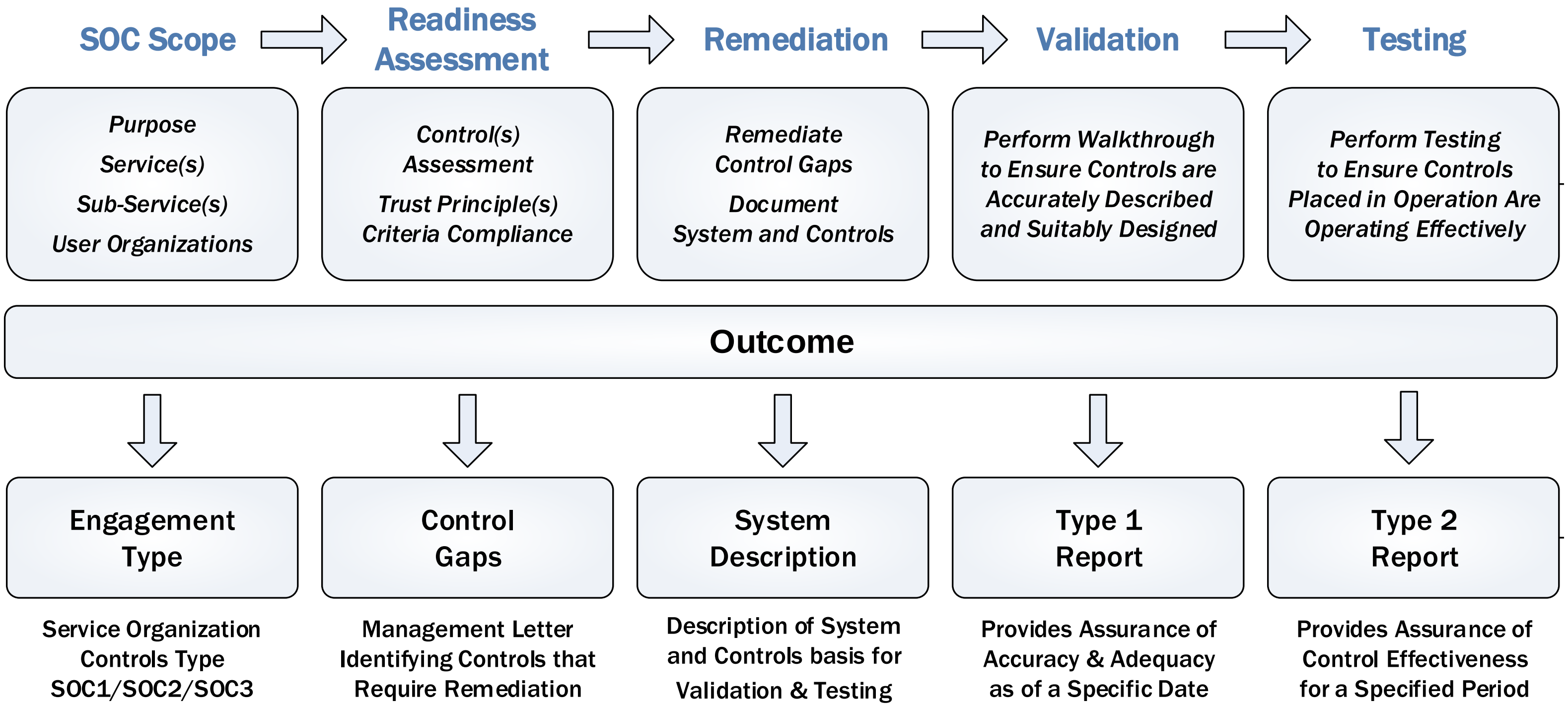
e. Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period

What Action To Take

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

SYSTEM AND ORGANIZATION CONTROLS (SOC) ENGAGEMENT STRATEGY



SOC Scope → Readiness Assessment → Remediation → Validation → Testing

Purpose

Service(s)

Sub-Service(s)

User Organizations

Control(s) Assessment

Trust Principle(s) Criteria Compliance

Remediate Control Gaps

Document System and Controls

Perform Walkthrough to Ensure Controls are Accurately Described and Suitably Designed

Perform Testing to Ensure Controls Placed in Operation Are Operating Effectively

Outcome

Engagement Type

Service Organization Controls Type SOC1/SOC2/SOC3

Control Gaps

Management Letter Identifying Controls that Require Remediation

System Description

Description of System and Controls basis for Validation & Testing

Type 1 Report

Provides Assurance of Accuracy & Adequacy as of a Specific Date

Type 2 Report

Provides Assurance of Control Effectiveness for a Specified Period

Create Opportunities

CLA exists to
create opportunities —
for our clients, our people,
and our communities.

CLAconnect.com

Mark Eich, CPA, CISA
Principal
612-397-3128
mark.eich@CLAconnect.com

Joel Eshleman, CISA, CIA
Director
717-558-0860
joel.eshleman@CLAconnect.com