Exploring Emerging Cyber Attest Requirements

With a focus on SOC for Cybersecurity

(“Cyber Attest”)
Introductions and Overview

- Audrey Katcher
  - Partner, RubinBrown LLP
  - AICPA volunteer: AICPA SOC 2 Guide Working Group and AICPA Assurance Services Trust/Data Integrity Task force
Companies will soon have new way to gut check cyber risk

TIMELY Discussion

SEC Spotlight

Cybersecurity

PCAOB
Public Company Accounting Oversight Board

Going forward, as noted in the Strategic Plan, PCAOB staff will continue to research the role of auditors with respect to fraud and potential emerging audit risk areas, such as cybersecurity.
Background

- Concept of third-party trust and independent assessment
- Increase in SOC 2 requests
- A greater need to understand entity-level cybersecurity as well
SOC 2 - Most Effective Way to Assess....

What is your most effective way to assess cloud provider risk?

- SOC 2 report (A) 48%
- CSA STAR report (B) 9%
- ISO27k certificate (C) 9%
- Onsite audit (D) 7%
- Send lengthy questionnaires (E) 17%
- Other (F) 10%

Total Results: 100

Source: RubinBrown

Cloud Security Assessments: You're Doing It Wrong!

RSA Conference 2017
San Francisco | February 13–17 | Moscone Center
History of IT and CPA Services

Source: Cybersecurity Attestation Examination Engagement
AICPA Auditing Standards Board, August 3, 2016
What’s New
SOC for Service Organizations

Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service

- SOC 1®—SOC for Service Organizations: ICFR
- SOC 2®—SOC for Service Organizations: Trust Services Criteria
- SOC for Service Organizations: SOC 2® HiTrust
- SOC for Service Organizations: SOC 2® CSA STAR Attestation
- SOC 3®—SOC for Service Organizations: Trust Services Criteria for General Use Report

New: SOC for Cybersecurity

A reporting framework through which organizations can communicate relevant useful information about the effectiveness of their cybersecurity risk management program and CPAs can report on such information to meet the cybersecurity information needs of a broad range of stakeholders

Under Development: SOC for Vendor Supply Chains

An internal controls report on a vendor’s manufacturing processes for customers of manufacturers and distributors to better understand the cybersecurity risk in their supply chains

Standards Considered

1. NIST Cybersecurity Framework or NIST CSF
2. International Organization for Standardization (ISO)/IEC 27001/27002 and related standards
4. FFIEC questionnaires
5. COBIT 5
6. COSO 2013 framework
7. HIPAA Security Rule
8. PCI DSS 3.1
9. NIST Special Publication 800 series
10. HITRUST CSF
## SOC Suite of Services

<table>
<thead>
<tr>
<th>Reporting Level</th>
<th>Report Category</th>
<th>Intended Audience</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| **Entity**      | **SOC for Cybersecurity** | ✓ Board  
✓ Management  
✓ Investor  
✓ Regulator  
✓ Analysts | Transparency regarding the entity’s cyber risk management |
| **Service Provider** | **SOC 2**  
(New guide coming) | ✓ Business unit management  
✓ Vendor risk management  
✓ Accounting / internal audit  
✓ CISO  
✓ BCP | Transparency for the services provided and provides assurance over the selected principles. with detail |
| **Service Provider** | **SOC 1**  
(Recently released guide) | Use of these reports is restricted to the management of the service organization, user entities, and user auditors. | Transparency for the services provided and provides assurance over internal control over financial reporting. with detail |
| **Supply Chain** | New guide coming | ✓ Business unit management  
✓ Vendor risk management  
✓ Accounting / internal audit  
✓ CISO  
✓ BCP | Transparency for the services provided and provides assurance over the selected principles. with detail |
Cybersecurity Risk Management Examination

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.

Note for this presentation: Due to the newness of the service and the Cybersecurity Guide not being released, there could be other considerations not discussed today or corrections needed to items presented.
Two sets of criteria

1. Description criteria used to prepare narrative of the cyber risk management program

2. Control criteria used to evaluate the effectiveness of controls in the program *

* May use other criteria such as the NIST Critical Infrastructure Cybersecurity framework and ISO 27001/27002 as control criteria as long as such criteria are appropriate for the engagement according to AICPA attestation standards.
A set of benchmarks to use when preparing and evaluating the presentation and description of the entity's cybersecurity risk management program (description).

A cybersecurity risk management program is the set of policies, processes and controls designed to protect information and systems from security events that could compromise the achievement of the entity’s cybersecurity objectives and to detect and respond to, mitigate and recover from on a timely basis, security events that are not prevented.
**Description Criteria**

- **Examination is in accordance with**
  - AT-C section 105 Concepts Common to All Attestation Engagements
  - AT-C section 205, Examination Engagements

- **Management is responsible for**:
  - Developing, implementing and operating the entity’s cybersecurity risk management program
  - Description of the entity’s cybersecurity risk management program
  - Assertion about whether the description is presented in accordance with the description criteria
  - Assertion about the effectiveness of the controls within the program based on a set of control criteria
Description Criteria

- May be used under consulting services (CS section 100, Consulting services: Definitions and Standards).

- Designed to permit management to describe entity-wide cybersecurity risk management program
  - May be used to apply to a limited portion of the entity
    - One or more specific business unit(s) / segment(s) which is (are) under an entity-wide or an independent cybersecurity risk management program
    - One or more specific sets of systems or particular sets of information used by the entity
Categories of Description Criteria

1. Nature of Business and Operations
2. Nature of Information at Risk
3. Cybersecurity Risk Management Program Objectives
4. Factors that have a significant effect on inherent cybersecurity risks
5. Cybersecurity risk governance structure
6. Cybersecurity risk assessment process
7. Cybersecurity communications and the quality of cybersecurity information
8. Monitoring of the cybersecurity risk management program
9. Cybersecurity control processes

Note, each category has 1-4 description criteria and several implementation guidance points
## Description Criteria and Related Implementation Guidance

### 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 |

**Implementation Guidance**

When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:

- *The entity’s principal markets, including the geographic locations of those markets, and changes to those markets*
Trust Services Criteria

- The control criteria used to evaluate and report on controls (suitability of the design and operating effectiveness) relevant to:
  - Security,
  - Availability,
  - Processing integrity,
  - Confidentiality, and/or
  - Privacy
Organization of Trust Services Criteria

- Aligned to the 17 criteria (known as principles) presented in “Internal Control – Integrated Framework, which was revised in 2013 by COSO.

- Includes supplemental criteria supporting:
  - Logical and physical access controls
  - System operations
  - Change management
  - Risk management
Trust Services Categories

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy
TSC generally not used when engaged to report on entity compliance with laws, regulations, rules, contracts, grant agreements.

Refer to / consider for the compliance engagement: AT-C section 105 and 315, Compliance Attestation
Trust Services Criteria

- AICPA Statements on Standards for Attestation Engagements
  - SSAE 18 (effective May 1, 2017)
  - AT-C 105, 205

- May be used under consulting services (CS section 100, Consulting services: Definitions and Standards.)
**Trust Services Criteria and Points of Focus**

(COSO not italics, TSC in italics, *system level only bold italics* *)

<table>
<thead>
<tr>
<th>TSP Ref. #</th>
<th>TRUST SERVICES CRITERIA AND POINTS OF FOCUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONTROL ENVIRONMENT</strong></td>
<td></td>
</tr>
<tr>
<td>CC1.1</td>
<td>COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.</td>
</tr>
<tr>
<td></td>
<td>The following points of focus highlight important characteristics relating to this criterion:</td>
</tr>
<tr>
<td></td>
<td>Points of focus specified in the COSO framework:</td>
</tr>
<tr>
<td></td>
<td>• Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.</td>
</tr>
</tbody>
</table>

* The font formatting serves as a key to the relative applicability.
Call to Action

1. Understand the standards and the terms

2. Evaluate the benefit to your organization

3. Prepare leadership for expectations in this type of reporting

4. Evaluate readiness
   - Perform an internal use only evaluation (under consulting standards)
Questions

Audrey Katcher, CPA, CISA, CITP
audrey.katcher@rubinbrown.com