2020 VIRTUAL ANNUAL MEETING & EXHIBIT

OCTOBER 26–29, 2020
System and Organization Controls (SOC) Audit: How to Appropriately Plan and Prepare for a Successful Audit

Rajeev Dutt, Milliman, Inc.
Amber Damergis, Milliman, Inc.
Binita Pradhan, BDO USA, LLP

October 29, 2020
SOCIETY OF ACTUARIES
Antitrust Compliance Guidelines

Active participation in the Society of Actuaries is an important aspect of membership. While the positive contributions of professional societies and associations are well-recognized and encouraged, association activities are vulnerable to close antitrust scrutiny. By their very nature, associations bring together industry competitors and other market participants.

The United States antitrust laws aim to protect consumers by preserving the free economy and prohibiting anti-competitive business practices; they promote competition. There are both state and federal antitrust laws, although state antitrust laws closely follow federal law. The Sherman Act, is the primary U.S. antitrust law pertaining to association activities. The Sherman Act prohibits every contract, combination or conspiracy that places an unreasonable restraint on trade. There are, however, some activities that are illegal under all circumstances, such as price fixing, market allocation and collusive bidding.

There is no safe harbor under the antitrust law for professional association activities. Therefore, association meeting participants should refrain from discussing any activity that could potentially be construed as having an anti-competitive effect. Discussions relating to product or service pricing, market allocations, membership restrictions, product standardization or other conditions on trade could arguably be perceived as a restraint on trade and may expose the SOA and its members to antitrust enforcement procedures.

While participating in all SOA in person meetings, webinars, teleconferences or side discussions, you should avoid discussing competitively sensitive information with competitors and follow these guidelines:

- Do not discuss prices for services or products or anything else that might affect prices
- Do not discuss what you or other entities plan to do in a particular geographic or product markets or with particular customers.
- Do not speak on behalf of the SOA or any of its committees unless specifically authorized to do so.
- Do leave a meeting where any anticompetitive pricing or market allocation discussion occurs.
- Do alert SOA staff and/or legal counsel to any concerning discussions
- Do consult with legal counsel before raising any matter or making a statement that may involve competitively sensitive information.

Adherence to these guidelines involves not only avoidance of antitrust violations, but avoidance of behavior which might be so construed. These guidelines only provide an overview of prohibited activities. SOA legal counsel reviews meeting agenda and materials as deemed appropriate and any discussion that departs from the formal agenda should be scrutinized carefully. Antitrust compliance is everyone’s responsibility; however, please seek legal counsel if you have any questions or concerns.
Presentation Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of the Society of Actuaries, its cosponsors or its committees. The Society of Actuaries does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented. Attendees should note that the sessions are audio-recorded and may be published in various media, including print, audio and video formats without further notice.
Presenter Bios – Milliman, Inc.

Rajeev Dutt, FSA, MAAA, CERA
Principal & Consulting Actuary

312-499-5572 (Office)
312-320-2213 (Mobile)
rajeev.dutt@milliman.com

- Over 25 years helping life insurance companies and retirement services organizations manage financial and control operational risks.

- Overseeing several Variable Annuity outsource programs, including market analysis, hedging financial risks, GAAP and Statutory reporting and projections, experience studies, M&A, and new product development.

- Responsibilities include managing the day-to-day operations to monitor and control P&L outcomes by developing a robust financial reporting platform emphasizing a quality and risk framework that aids client organizations in effectively executing on their risk management policies.
Amber Damergis  
Principal & Senior Director  
Head of Governance & Risk Management  

312-279-3089 (Office)  
amber.damergis@milliman.com

- Over 15 years of experience in the areas of governance, risk, and compliance, Amber is a Principal & Senior Director at Milliman, Inc.
- Trusted partner to over 40 managed services clients by supporting a robust and comprehensive control framework that satisfies clients’ regulatory, compliance, and board-mandated requirements.
- Oversees multiple external audit engagements related to internal controls over financial reporting for multi-national clients.
- Successfully on-boarded over 40 managed services clients into the SOC 1 control framework at Milliman.
- Trusted advisor on effective risk identification and control design.
Binita Pradhan, CPA, CISA
Partner

415-490-3120 (Office)
510-290-8603 (Mobile)
bpradhan@bdo.com

- With over 20 years of experience in the areas of risk and compliance, Binita is a partner at BDO USA, LLP.
- Subject matter expert on third party attestation (SOC) services serving on the AICPA SOC Supply Chain Task Force that authors SOC for supply chain guides; and the AICPA SOC 2 Task Force that authors SOC 2 guides.
- Known for her hands-on style and effective communications and deep trusted advisor relationships with client executives, related to security, cyber, privacy, cloud, business processing. Some of Binita’s clients are Milliman Inc., Palo Alto Networks, Symantec, Adobe, and many others.
- Experience working with a wide range of industries including technology, insurance, manufacturing and distribution, financial services, healthcare, and governmental organizations.
Objectives

- Benefits of a SOC Audit
- SOC 1, SOC 2, SOC 2\(^+\) and SOC 3 overview, and
- How to prepare for a SOC examination
BENEFITS OF SOC REPORTS – THE WHY
Why Audits Matter

Auditor reports provide independent and objective assurance of an organization’s operations, both in terms of how business is conducted and what precautions the organization takes to protect its information assets. Audits help to improve an organization’s effectiveness in their risk management efforts while also providing current clients comfort over the organizations to which they have outsourced their services or have dependencies. Additionally, prospects often look for certifications (e.g., ISO or HITRUST) to further reinforce trust and provide transparency in an organization’s risk management framework.
Audit Stakeholders

Individuals at the company that support the work product and/or deliverable(s); this includes business process as well as the technology being leveraged. Examples include:

- Data transformation
- Data validation and completeness
- Reporting (e.g., financial, attribution, etc.)
- Trading
- Trade reconciliations and margin movement
- Software development and maintenance of models and applications
- Logical Access
- Network Security
- Data Backup
- Physical Security
Life with SOC

- Third-party compliance **must-have**

- Service providers offer clients **assurance**

- SOC reports have become the **market standard** for third party attestation

  → Serves as a **powerful testament** to company’s commitment to sound operating practices and the ability to meet regulatory, compliance, and market demands

- **Prerequisite** in order to advance in the sales discovery and transaction processes
The SOC Results

Efficient

Cost effective

Customer trust
Section Summary

Sell the benefits of SOC reports to the process owners. This will result in a *streamlined effort*, *reduced stress*, and build a *collaborative* program.
SOC OVERVIEW
SOC Reporting Landscape

SOC 1
SOC for Service Organizations

SOC 2
SOC for Cybersecurity

SOC 3
SOC for Supply Chain (new)

System and Organization Controls (SOC)
SOC 1 Reports

- Standard - SSAE 18

- Controls at a service organization relevant to user entities' internal control over *financial reporting*

- Intended Users - Auditors of the user entity’s financial statements, management of the user entity and management of the Service Organization
Type 1 Reports

- Type 1 – report on:
  - fairness of the presentation of management’s description, and
  - suitability of the design of the controls
Type 2 Reports

- Type 2—report on:
  - fairness of the presentation of management’s description, and
  - suitability of the design and operating effectiveness of the controls
SOC 2 Reports

- Standard – SSAE 18; AT-C Section 105 and 205

- Evaluates an organization’s information systems relevant to Trust Service Categories and related criteria

- Intended Users - User entity personnel and select others that wish to obtain an understanding of controls at a service organization related to one or more trust services categories
## SOC 2 Reports (Cont’d)

<table>
<thead>
<tr>
<th>Category</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Information and systems are protected against unauthorized access, unauthorized disclosure of information and damage to systems that could compromise the availability, integrity, confidentiality and privacy of information or systems and affect the entity’s ability to meet its objectives.</td>
</tr>
<tr>
<td>Availability</td>
<td>Information and systems are available for operation and use to meet the entity’s objectives.</td>
</tr>
<tr>
<td>Processing Integrity</td>
<td>System processing is complete, valid, accurate, timely and authorized to meet the entity’s objectives.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Information designated as confidential is protected to meet the entity’s objectives.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Personal information is collected, used, retained, disclosed and disposed to meet the entity’s objectives.</td>
</tr>
</tbody>
</table>
SOC 2+

- Increases the utility of a SOC 2 report and overall compliance costs and efforts.

- Effective option to help streamline compliance efforts for service organizations subject to multiple regulatory standards.
SOC 2⁺ (Cont’d)

Overlap with SOC 2 and some combination of other major standards, including, but not limited to:

- HITRUST
- HIPAA
- NIST SP-800-53 R4
SOC 3

- Standard - SSAE 18; AT-C Section 105 and 205

- Intended Users - SOC 3 reports are general use reports. Any users who want assurance on controls at a Service Organization related to TSP, but do not have the need for the level of detail provided in a SOC 2 report.
Section Summary

- SOC 1 - Auditor-to-auditor communication
- SOC 2 - Restricted use
- SOC 3 - General use
- SOC 2\(^+\) achieve the elusive goal of “audit once, report many”
HOW TO PREPARE FOR A SOC EXAMINATION
Preparing for an Audit

Understand Applicability

Identify Scope

Define Processes and Controls
Preparing for an Audit

Lifecycle of an Audit

Confirm audit scope, identify stakeholders, and confirm processes and controls are up-to-date, establish expectations with stakeholders and auditors.

Provide audit report to relevant interested parties and any other supplementary documentation.

Schedule onsite walkthroughs with applicable process owners and testing and collect and hand over requested evidence.

Review and confirm any exceptions noted by third-party auditors and determine remediation plan if required.
Preparing for an Audit
Planning & Scoping

Audit Planning Checklist

✓ Are key stakeholders involved and are they attuned to the information that has been provided to the auditors?

✓ Have clear expectations and limitations been established? Information provided should be relevant, appropriate, and measured.

✓ Is there a clear understanding of the scope between the stakeholders and the auditors and does this scope make sense? There should be agreement on the focus of the audit.

✓ Have the onsite visit timeline and agenda been defined and have logistics been considered?

✓ Have you had prep meetings with stakeholders to review expectations and the do’s and don’ts?

✓ Have you consulted with your audit, compliance, and risk professionals?
Preparing for an Audit
Onsite Fieldwork

- Have a kick-off meeting and establish guidelines
- Be clear on audit scope and ensure all stakeholders are prepared
- Secure a location for the auditors to work that limits open exposure to sensitive areas
- Prepare all sensitive items that can only be viewed onsite and have them readily available
- Offense is the best defense; answers should be clear and concise
- Be transparent
During and After the Audit

Exception Vetting and Remediation

Regular Check-Ins
- Establish regular check-ins with the auditors to stay apprised of progress and findings

Vetting Responses
- Vet responses with all stakeholders before providing to the auditors

Remediation Validation
- If remediation of exceptions is necessary, ensure solutions are sustainable and demonstrative
Section Summary

- Lifecycle
- Planning
- Fieldwork
- Vetting and Remediation