CONTRACTS
The Upside of Risk

HOW TO LEVERAGE SOC AND SSAE 18 REPORTS

THROUGHOUT EVERY DEPARTMENT OF YOUR FINANCIAL INSTITUTION

CONTRACTS 1

1

AGENDA

- Responsibility to review
  - Importance of the reports to various department heads
- Correlation with risk management
  - What SOC reports mean to various aspects of the organization (i.e. IT/info Security and Vendor Management)
- SOC report results – effect on the organization
  - Appropriateness of internal controls in place at the TSP
- What is the risk of ignoring SOC content
- The W's of a SOC report
- Different types of SOC reports
- Contents of a SOC report
- Purpose of the SOC report
- Is SOC information reliable
- Educational resources

CONTRACTS 2

2

RESPONSIBILITY TO REVIEW

- Who is responsible in the financial institution to review the information? Or even only understand the overall content
  - Owner of the product / service being provided by the TSP / vendor
    - Departments / Lines of Business
  - Operations Officer
  - Information Technology (ISO, Applications Support, Product Support)
  - Compliance
    - Addressing compliance risks associated with the product / service
  - Risk Management
  - Executive Team
  - Board of Directors

3

RESPONSIBILITY TO REVIEW

- Per the AICPA, the following parties should have access to and review SOC reports:
  - Parties that are knowledgeable about:
    - the nature of the service provided by the service organization
    - how the service organization's system interacts with user entities, subservice organizations, and other parties
    - internal control and its limitations
    - the criteria and how controls address those criteria

4

CORRELATION WITH RISK MANAGEMENT

- How do the different types of SOC reports and the content within each type correlate with risk management?

- Four pillars of risk management*
  1. Identify
     - Categorical Risk - Risks inherent in the relationship of a TSP / vendor may be in one or more risk categories
  2. Measure
     - Initial/inherent Risk
  3. Mitigate
  4. Monitor

*Per FFIEC IT Examination Handbook – Management – IT Risk Management

5

CORRELATION WITH RISK MANAGEMENT

OPERATIONAL RISK

- Outsourced IT services can contribute to operational risks (also referred to as transaction risks). Operational risk may arise from fraud, error, or the inability to deliver products or services, maintain a competitive position, or manage information. It exists in each process involved in the delivery of the financial institutions' products or services. Operational risk not only includes operations and transaction processing, but also areas such as customer service, systems development and support, internal control processes, and capacity and contingency planning

6

CORRELATION WITH RISK MANAGEMENT - IDENTIFY

REPUTATION RISK

- Errors, delays, or omissions in information technology that become public knowledge or directly affect customers can significantly affect the reputation of the serviced financial institutions. For example, a TSP's failure to maintain adequate business resumption plans and facilities for key processes may impair the ability of serviced financial institutions to provide critical services to their customers.

7

CORRELATION WITH RISK MANAGEMENT - IDENTIFY

STRATEGIC RISK

- Inadequate management experience and expertise can lead to a lack of understanding and control of key risks. Additionally, inaccurate information from TSPs can cause the management of serviced financial institutions to make poor strategic decisions.

8

CORRELATION WITH RISK MANAGEMENT - IDENTIFY

COMPLIANCE (LEGAL) RISK

- Outsourced activities that fail to comply with legal or regulatory requirements can subject the institution to legal sanctions. For example, inaccurate or untimely consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose the institution to civil money penalties or litigation. TSPs often agree to comply with banking regulations, but their failure to track regulatory changes could increase compliance risk for their serviced financial institutions.

9

CORRELATION WITH RISK MANAGEMENT - IDENTIFY

INTEREST RATE, LIQUIDITY, AND PRICE (MARKET) RISK

- Processing errors related to investment income or repayment assumptions could lead to unwise investment or liquidity decisions thereby increasing market risks.

10

CORRELATION WITH RISK MANAGEMENT - MONITOR

- Through information contained within independent audits, an understanding of strengths and weaknesses as they relate to the controls in place to mitigate various risks

11

CORRELATION WITH RISK MANAGEMENT – CONTROL / MANAGE

Applying the understanding of controls and their effectiveness to make informed decisions

- to maintain in a business as usual environment,
- maintain a relationship with the TSP / vendor but with additional controls adopted and implemented at the FI, or
- discontinue the relationship due to breach/violation of contract

12

SOC REPORT RESULTS – EFFECT ON THE ORGANIZATION

What aspects of an organization are affected by the results within a SOC review and what are some actions that may be warranted based on results?

- All –
  - The effectiveness or ineffectiveness of products / services offered through the TSP / vendor relationship will impact (positively/negatively) the FI's strategic plan and related strategic objectives and initiatives

13

SOC REPORT RESULTS – EFFECT ON THE ORGANIZATION

IT – INFORMATION SECURITY

- The controls in place at the TSP / vendor for products and services provided to the FI and the effectiveness of those controls affect the FI's residual risk. Information regarding the effectiveness or non-effectiveness of controls should be understood and included within the FI's information security risk assessment. Updates to the risk assessment should take place on any occasion where updated information is communicated or known.
- Controls in place at TSPs / vendors related to the protection of sensitive or private information should be addressed (at minimum at a high level) within the organization's information security program.

14

SOC REPORT RESULTS – EFFECT ON THE ORGANIZATION

IT – CYBERSECURITY

- In the cybersecurity assessment tool, when identifying the FI's "Maturity," questions are asked regarding the controls in place to mitigate various risks.

Domain 1 – Cyber Risk Management and Oversight

- Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate committee at least annually. In order to provide an up to date and factual representation of Information Security status the FI must include information obtained regarding the controls in place and the effectiveness of those controls at the TSP / vendor.

SO…WHAT'S THE RISK?

What is the risk of ignoring SOC content?

- Acceptance of risk and its impact on the organization – Not understanding your TSP / vendor's ability to address and mitigate risk would mean you accept any additional risk as a result of the TSP / vendor's mismanagement of risk.

- Acceptance of varying delivery standards and its impact on the organization – Not understanding controls and their effectiveness would mean the acceptance of changes in a product/service delivery, dependability, quality.

THIRD-PARTIES AMPLIFY CYBER RISK

- "On average, organizations **spent $10 million responding to third-party breaches** over a 12-month period in 2016." CSO Online | 2016
- "Only 35% of enterprise security professionals are very **confident in knowing the actual number of vendors** accessing their systems." Bomgar survey | 2016
- "Just 34% **know the number of individual log-ins** that can be attributed to vendors." Bomgar survey | 2016
- "Over **60% of data breaches** can be linked either directly or indirectly to a third party." Soha Systems | 2016

THIRD-PARTIES AMPLIFY CYBER RISK

- "94.3% of executives have **low to moderate confidence in their third-party risk management** tools and technology, and 88.6% have low to moderate confidence in the quality of the underlying risk management processes." Deloitte | 2017
- "The estimated **direct source of security incidents from third-party vendors was 19% in 2017**." PwC | 2017
- "**Only 52% of companies have security standards for third-parties**." PwC | 2018

BOARD AND LEADERSHIP RESPONSIBILITIES

- Every year (starting on February 15, 2018) either the chairperson of the board or a senior officer will be required to sign a statement that he/she has reviewed all the applicable documents about their company (and about their vendors) that are necessary to certify compliance with the Rules during the prior year.
  - The company actually needs to have met the Rule's requirements over the prior year.

19

THE W'S OF A SOC REPORT

- **What is a SOC report**
  - SOC = System and Organizational Controls
  - Third-party audit to determine the status and reliability of internal controls
- **Who performs a SOC review?**
  - Independent auditors who are not employees of either the technology service provider (TSP) or the serviced institution(s) (Financial Institution - FI)
- **Why are SOC reviews initiated by the vendor?**
  - A TSP (vendor) is subject to separate audits by internal auditors from each of the serviced institutions. These audits may duplicate each other, creating a hardship on the provider's (TSP / vendors) management and resources; therefore, the vendor, to reduce burden, arranges its own third party audit.

20

DIFFERENT TYPES OF SOC REPORTS

SERVICE ORG CONTROL 1 (SOC 1)	SERVICE ORG CONTROL (SOC 2)	SERVICE ORG CONTROL 3 (SOC 3)
Restricted Use Report	Restricted Use Report	General Use Report
Type 1 or Type 2	Type 1 or Type 2	(No types)
Purpose: Reports on controls for financial statement audits	Purpose: Reports on controls related to compliance and/or operations	Purpose: Reports on controls related to compliance and/or operations

Trust Services Principles and Criteria

DIFFERENT TYPES OF SOC REPORTS

Type 1 Reports will include the following content:

- Description of the service organization's system
- Assertion from management of the service organization that fairly presents the service organization's system as designed and implemented **as at the specified date**, and that the controls related to the control objectives stated in the description of the "system" for the service organization were suitably designed to achieve the control objectives **as of the specified date**.
- Service auditor's assurance report

- Main Difference is that Type 2 covers a period of time
- Industry views Type 2 associated with more mature and stable controls

HOW DO SSAE 16 & 18 FIT IN?

SSAE = Statement on Standards for Attestation Engagements

SSAE 16's and 18's are application of the standards set forth in completing a SOC (System and Organizational Controls).

The standard with which a SOC report was completed.

- Provides management and user entities with an opinion on:
  - Fair presentation of the system description,
  - Controls related to the control objectives are suitably designed, and
  - Controls related to the control objectives are operating effectively.

CONTENTS OF A SOC REPORT

- Title of Report
- Auditors Opinion
- Scope of Report
- Company Assertion
- Body of Report
- User Entity Controls or Complementary Controls
- Complimentary Third-party Organizational Controls
- Testing
- Company Additional Information

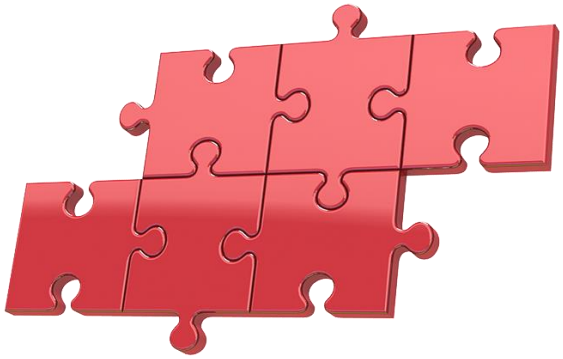
PURPOSE OF SOC REPORTS

Relied upon for assurance:

- Verify from a third party audit that appropriate controls exist

- Scope
  - Defines work

- Exceptions
  - How corrected



CONTRACTS

25

RELIABILITY

- Should the FI rely on information within a SOC review that is provided by the vendor (TSP)?
  - Is the independent auditor qualified to perform the review?
  - Does the scope satisfy the FI's own audit objectives?
    - Audit objectives would include addressing those risks inherent in the products and services offered by the vendor (TSP)
  - Significant deficiencies reported are corrected

CONTRACTS 26

26

EDUCATIONAL RESOURCES

- Educational resources:
  - Ncontracts - https://ncontracts.com/ssae-18/
  - FFIEC – Federal Financial Institution Examination Council
  - ISACA - Information Systems Audit and Control Association
  - AICPA – American Institute of CPAs

CONTRACTS
The Upside of Risk

Subscribe to get free Risk and Vendor Management content in your inbox!

https://ncontracts.com/blog