2023 INTERNAL AUDIT WEBINAR SERIES

COURSE 4

# BEST PRACTICES FOR INTERNAL AUDIT RELATED TO SOC REPORTING

October 24, 2023

2023 INTERNAL AUDIT WEBINAR SERIES

# BDO and Our Internal Audit Webinar Series

# Jamey Loupe, CISA, CCSK

## MANAGING DIRECTOR, DATA RISK & CONTROLS, RISK ADVISORY SERVICES

Jamey Loupe is a Managing Director in BDO's Risk Advisory Services practice where he focuses on IT risk advisory strategies. He has more than 15 years of progressive experience leading and organizing teams and projects and has provided audit and advisory services to various Fortune 500 and mid-size multinational companies in multiple industries. Prior to joining BDO, Jamey worked in the internal audit and information technology (IT) security functions for oil and gas services companies. Prior to that he was with a Big Four Firm. His experience includes:

- Leading, managing and conducting IT internal audits
- Managing complex IT Sarbanes-Oxley (SOX) compliance projects
- Recommending and implementing IT process improvements
- Conducting and leading enterprise resource planning (ERP) pre- and post-implementation reviews
- Conducting IT security assessments

### EDUCATION

- Cybersecurity Certificate, Harvard University
- M.L.A., Information Management Systems, Harvard University Extension
- B.A., Information Systems Decision Sciences, Louisiana State University

### PROFESSIONAL AFFILIATIONS

- Institute of Internal Auditors (IIA)
- Information Systems Audit and Control Association (ISACA)
- Cloud Security Alliance (CSA)
- Marine Corps Association and Foundation (MCA&F)

713-407-3935
jloupe@bdo.com

# Matt Behan, CPA

## DIRECTOR, DATA RISK & CONTROLS, RISK ADVISORY SERVICES

Matt Behan is a Director within the Risk Advisory Services group at BDO USA. He has more than 10 years of progressive experience leading and organizing teams and projects. He has provided audit and advisory services to various Fortune 500 and mid-size multi-national companies in multiple industries. Prior to joining BDO, Matt worked in the Technology Risk group as part of a Big Four firm's Business Consulting practice.

Throughout his career, Matt has worked on Internal Audits, Financial Statement Audits (for both private and SOX 404 clients), Controls Optimization Evaluations, Service Organization Controls (SOC) evaluations, System Implementations, Vendor Risk Assessments, Policy Governance Assessments, and SOX 404 readiness assessments. Matt also has experience with numerous applications and systems including SAP, SAP S/4 HANA, Oracle, PeopleSoft, Infor Lawson, NetSuite, Workday, Epic, Windows, SQL, and Unix/Linux.

312-730-1285
mbehan@bdo.com

### PROFESSIONAL AFFILIATIONS

- American Institute of Certified Public Accountants (AICPA)
- Illinois CPA Society (ICPAS)
- Institute of Internal Auditors (IIA)

### EDUCATION

- B.A., Accounting, Indiana University
- M.S., Information Systems, Indiana University

# Learning Objectives

**At the conclusion of this session, attendees will be able to:**

Define the Basics of SOC Reports and Their Purpose

Describe Potential Impacts on SOX Audits with SOC Report Reliance

Identify Internal Audit's Obligations Related to SOC Reporting

Describe How to Evaluate Third-party Vendor Risk Through the Use of SOC Reports

2023 INTERNAL AUDIT WEBINAR SERIES

# General Background

# General Background

- System and Organization Controls (SOC) for Service Organizations reports are designed to help service organizations that provide services to other entities, build trust and confidence in the service performed and controls related to the services through a report by an independent CPA. Each type of SOC for Service Organizations report is designed to help service organizations meet specific user needs:
  - **SOC 1:** ICFR – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
  - **SOC 2:** Trust Services Criteria – Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
  - **SOC 3:** Trust Services Criteria for General Use Report
- Report standards are set by the American Institute of Certified Public Accountants (AICPA)

# Report Types and Key Differences

| REPORT | WHO - AUDIENCE | WHY - PRIMARY USE | WHAT - CONTENT | HOW - DISTRIBUTION |
|---|---|---|---|---|
| SOC 1 | ▶ Controller's Office<br>▶ External Auditors | ▶ Financial Statement Audit<br>▶ SOX 404 | Controls relevant to internal controls over financial reporting | Restricted to user entities and their auditors for use in financial statement audits and related matters |
| SOC 2 | ▶ Regulators<br>▶ Customers and Business Partners | ▶ Vendor management programs<br>▶ Internal risk management processes<br>▶ Regulatory oversight<br>▶ Limited audit use (ITGCs only) | Concerns regarding:<br>▶ Security<br>▶ Availability<br>▶ Processing Integrity<br>▶ Confidentiality<br>▶ Privacy | Restricted to users with "sufficient knowledge" and understanding of the service organization and internal controls (e.g., current and prospective customers, business partners, regulators, employees) |
| SOC 3 | ▶ General Public | ▶ Initial vendor due diligence | SOC 2 high level summary without the detailed controls and results necessary for a full review | General use – No restrictions |

# Report Types and Key Differences

| TYPE 1 | TYPE 2 |
| --- | --- |
| ▶ Controls designed and implemented **at a point in time** | ▶ Designed **and** operating effectiveness of controls **throughout a period of time** |
| ▶ Dated “as of” a particular date | ▶ Covers a period of time |
| ▶ Walkthrough of process/control design only | ▶ Walkthrough of design and testing of operating effectiveness to provide reasonable assurance control objectives or specified criteria are met |

# Other SOC Report Types

| REPORT | WHO - AUDIENCE | WHY - PRIMARY USE | WHAT - CONTENT | HOW - DISTRIBUTION |
|---|---|---|---|---|
| **SOC for Cyber** | ▶ General Users | ▶ Confidence regarding effectiveness of cybersecurity controls | Controls regarding cybersecurity risk management program | General use – No restrictions |
| **SOC for Supply Chain** | ▶ Management<br>▶ Specified parties | ▶ Stakeholder trust over key aspects of production, manufacturing, or distribution operations | Controls of production, manufacturing or distribution processes | Restricted to the use of the entity and specified parties, including customers and business partners with knowledge of the nature of goods and internal controls |

# SOC Report Impact on Audits

- Companies often outsource aspects of their operations to Service Organizations.
- Service Organizations can perform a variety of services ranging from executing a specific task on behalf of the Company to replacing entire business units or functions.
- Although many Service Organizations may be used by a Company, not all may be relevant to a SOX audit.
- Services are relevant to a SOX audit when those services, or the controls over the services, impact the Company's information systems, including those relating to business processes, relevant to financial reporting.
- When a service is deemed relevant, the Company should inquire about the availability of a SOC report covering the specific services.
- Once obtained, the Company should analyze the report and report results.

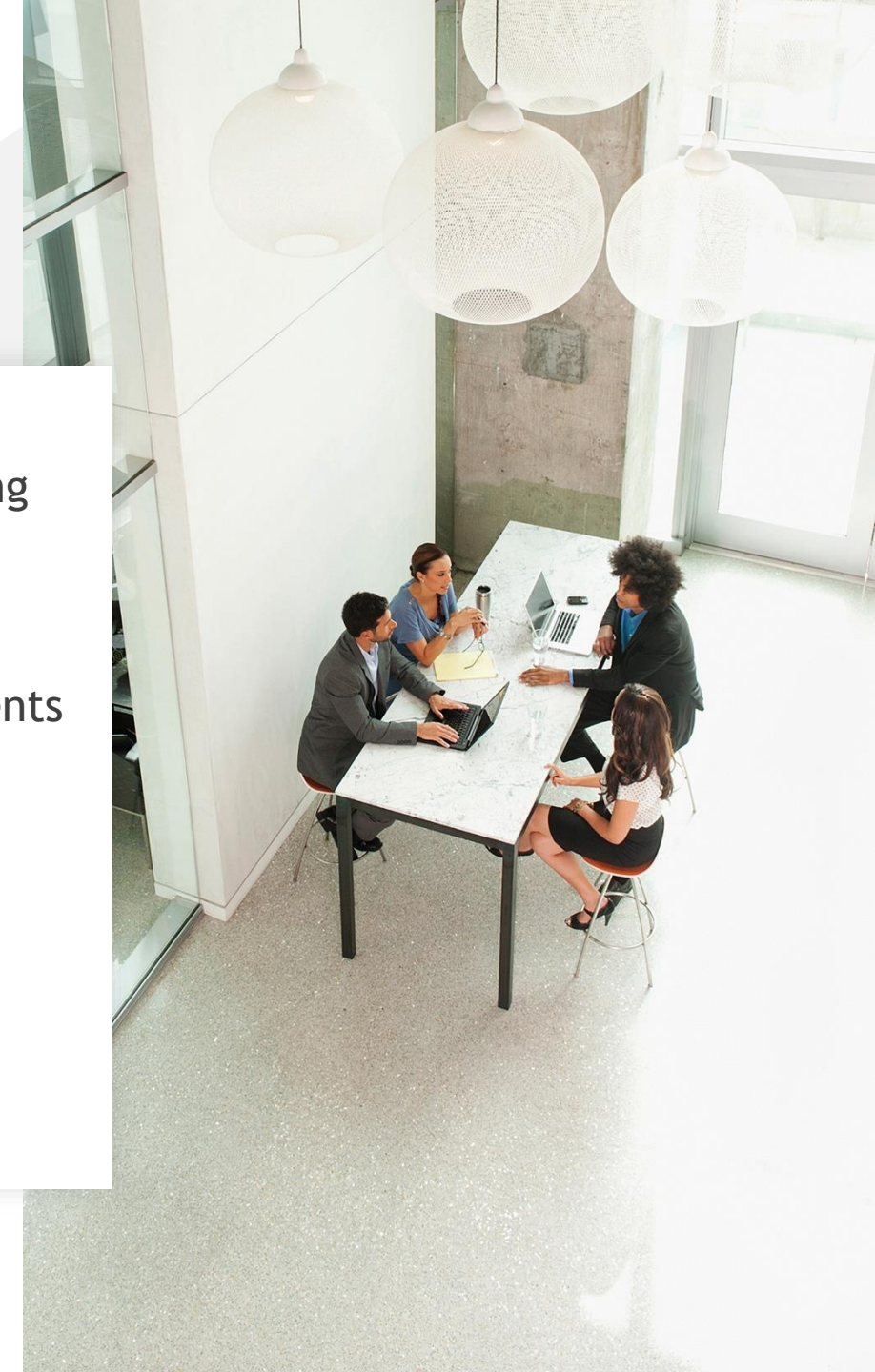
2023 INTERNAL AUDIT WEBINAR SERIES

# Benefits of SOC Reports

# Third-Party Risk Management

Third-party risk management refers to the process of identifying, assessing, and mitigating the risks associated with engaging and relying on third-party vendors, suppliers, contractors, or service providers. It involves implementing strategies and controls to ensure that the organization's operations, data, and reputation are protected from potential risks arising from these external relationships. Key components and steps involved in third-party risk management include:

- Vendor Selection and Due Diligence
- Risk Assessment
- Contractual Agreements
- Ongoing Monitoring



# Risk Assessment and Contractual Agreements

Once a vendor is selected, a comprehensive risk assessment should be conducted to identify and evaluate the potential risks associated with the vendor's services. This assessment should consider factors such as data security, operational resilience, regulatory compliance, and business continuity.

Clear and well-defined contractual agreements should be established with the vendor. These agreements should outline the responsibilities, obligations, and expectations of both parties, including provisions related to data protection, confidentiality, service levels, and dispute resolution.

Utilizing the vendor’s SOC report and requiring the vendor to continuing maintaining SOC certifications via contractual SLAs can further reduce risk throughout the length of your relationship with the vendor.

# Vendor Selection and Due Diligence

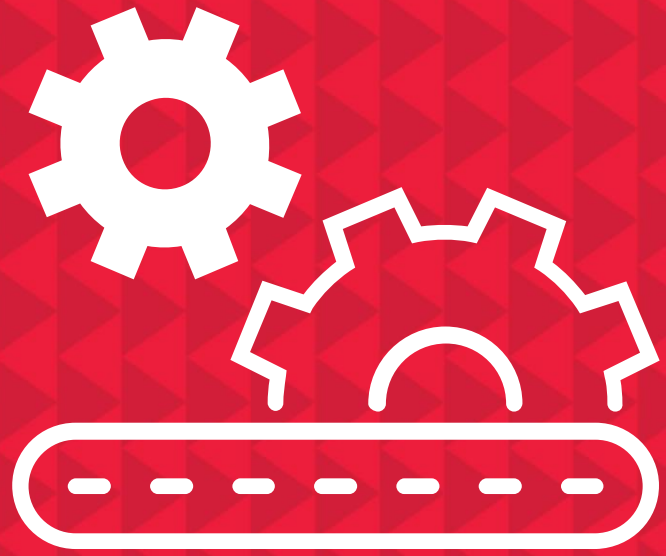
- This step involves conducting a thorough evaluation of potential vendors before engaging in a business relationship. It includes assessing their financial stability, reputation, compliance with regulations, security practices, and any potential conflicts of interest.
- SOC Reports can be requested and obtained to ensure the potential vendor has the adequate controls in place to protect the organization's data and operations.

# Ongoing Monitoring

- Regular monitoring of the vendor's performance and compliance is essential to ensure ongoing risk mitigation. This can include periodic assessments, audits, and reviews of the vendor's controls, policies, and procedures. It is important to establish mechanisms for reporting and addressing any identified issues or breaches promptly.
- The simplest way to perform ongoing monitoring is to regularly obtain the vendor’s SOC report (at least annually) and perform the analysis outlined earlier in this presentation.

2023 INTERNAL AUDIT WEBINAR SERIES

# Assessing a SOC Report



# Report Review Guidance

**When performing a review of System and Organization Control (SOC) reports for organizations providing services to a client, Management should consider the following key areas:**

- Initial Report Details
  - Report Type (1 or 2)
  - Coverage Period
  - Bridge Letter
- Service Auditor's Opinion
- Management's Assertion
- System Description
- In-Scope Applications
  - Control Design Details
  - Complementary User Entity Controls (CUECs)
  - Complementary Subservice Organization Controls (CSOCs)
- Tests of Operating Effectiveness
  - Control Operating Conclusion
  - Management's Responses to any Deviations
- Additional Information Provided by Management

# Initial Report Details

**On the cover page of each SOC report , you should find high level details that can help you on your initial assessment of the report:**

- **Report Title:** will be the high-level description of the services analyzed within the SOC report. The Company will want to validate this matches its expectations based on the services it receives from the Service Organization. The Company will also want to identify if the report is a SOC 1 or a SOC 2. Both can be used to support a SOX audit, but SOC 2 gives **ITGC support only.**
- **Report Type (1 or 2):** the type of report will be indicated: a Type 1 or a Type 2 report. Type 1 reports are design on**ly** and should not be used in support of a SOX audit.
- **Coverage Period:** details the period that the Service Organization's audit performed testing. The Company will want to match this against its audit period and assess gaps, as necessary.
- **Bridge Letter:** though not part of the cover page, this will be provided by the Service Organization upon request. This will provide additional coverage should there be a gap in the coverage period. The Company should minimize the amount of time reliance is placed on a bridge letter (typically three months or less).

# Identify the Scope of the SOC report

## Soc 1 and Soc 2 Reports Are Clear as to the Scope

Additional Scope Considerations:

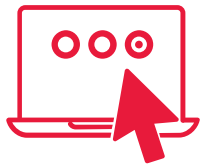
Specific Locations

Certain Date or Timeframe

Systems Involved

Subservice Organizations

Responsible Staff Members



Business Applications and Technology Platforms Covered

Processes That Focus on Internal Control Over Financial Reporting

SECTION 1

# Service Auditor's Opinion

- The first section of each SOC report will be the Service Auditor's Opinion.
- This section provides details on the Service Auditor themselves, their scope and limitations, and their opinion on the overall control environment.
- The Company will want to analyze the opinion for:
  - **Service Auditor Competency:** identify whether the Service Auditor is a reputable organization in good standing with the AICPA or other professional bodies.
  - **Scope and Limitations:** determine of the scope detailed by the Service Auditor matches what is expected by the Company and, if any exists, if the limitations identified by the Service Auditor impact the Company's ability to rely on the report.
  - **Auditor Opinion:** inspect the Opinion section for the Service Auditor's overall opinion. This section should detail whether the Service Auditor has modified their opinion in any way. The Service Auditor will indicate this by using the words "qualified" or "except for" when detailing the effectiveness of controls.

# Types of Opinions

## UNQUALIFIED

The auditor fully supports the findings, with no modifications; controls met requirements demanded by AICPA SOC guidance.

- The auditor may use “unqualified” to describe the opinion if it includes an emphasis-of-matter paragraph (widely used by auditors in their reports when they consider it is necessary to draw attention to a certain issue; it would not modify the opinion of the auditor, but simply highlight a situation of relevance).

## OTHER

The auditor must express their opinion in one of the following ways:

- Qualified opinion: The auditor cannot express an unqualified opinion; however, the issues are not pervasive.
- Adverse opinion: The auditor believes that there are material and pervasive issues. Report readers should not rely on the vendor’s system.
- Disclaimer of opinion: The auditor is unable to express an opinion due to insufficient evidence, and the possible effects could be both material and pervasive.

SECTION 2

# Management's Assertion

- The second section of each SOC report is Management's Assertion.
- This section provides details from Management of the Service Organization, asserting that they believe they have an effective control environment in relation to the control objectives (SOC 1) or principles (SOC 2) audited against.
- The Company will want to analyze the assertion to determine whether it aligns with expectations on the **services received** and that management has not flagged any known system deficiencies that would impact supporting the control environment.

SECTION 3

# System Description

- The third section of each SOC report is the System Description. This section is generally fully owned by the Service Provider.
- This section provides details on the services provided, in-scope systems, detailed narratives about the control environment, and references to any carved-out subservice organizations, complementary user entity controls, and subservice organization controls.
- The Company will want to analyze the System Description for:
  - **Systems and Services:** ensure the system the Company uses is adequately covered by the report provided. Service Providers often have multiple SOC reports, so it is important to validate you have the correct report.
  - **Complementary User Entity Controls (CUECs):** identify if there are any CUECs that impact the Company's control environment.
  - **Complementary Subservice Organization Controls (CSOCs):** identify if there are any CSOCs that impact the Company's control environment.

SECTION 3

# Complementary User Entity Controls

- Complementary User Entity Controls (CUECs) are controls that the Service Provider has included within its system description that rely on the Company to implement in order to achieve the Service Provider's control objectives.
- Generally, CUECs are found at the end of Section 3. On rare occasions, they may be placed within the controls in Section 4.
- The Company will want to analyze the CUECs for:
  - **Relevancy:** determine whether the individual CUEC is applicable to the Company's environment. If not, provide details on why it is not applicable.
  - **Control Mapping:** if a CUEC is applicable, the Company will need to map it to an internal control. It is best practice to treat these in-scope CUECs as if they were any other internal control wholly owned by the Company.
  - **Example CUECs:** most reports will require some sort of user authentication controls (passwords, new users, user reviews) and change testing controls.

SECTION 3

# Complementary User Entity Controls and Examples

## Complementary User Entity Controls (CUECs)

ABC's controls relating to its security management and support services system cover only a portion of the overall internal control for each user entity of ABC. It is not feasible for the control objectives relating to the security management and support services system to be solely achieved by ABC. Certain control objectives specified in the description can be achieved only if CUECs contemplated in the design of ABC's controls are suitably designed and operating effectively, along with controls at ABC. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with ABC's controls, taking into account the related CUECs identified below, where applicable. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control structure to determine whether identified CUECs have been implemented and are operating effectively.

| Number | CUECs | Applicable Control Objective |
|---|---|---|
| 1. | User entities are responsible for establishing account restrictions, compliance rules, proxy voting elections, trade requests, and reporting requirements. | CO1 and CO2 |
| 2. | User entities are responsible for communicating account changes and changes in authorized advisors to ABC. | CO4 |
| 3. | User entities are responsible for providing accurate bank account information and preferences for funding and distribution purposes. | CO3 |
| 4. | User entities are responsible for communicating changes in access to the ABC client portal. | CO12 |

SECTION 3

# Complementary Subservice Organization Controls

- When the carve-out method is used for presenting a subservice organization, the controls performed by the subservice organization are referred to as complementary subservice organization controls (CSOCs).
- Generally, CSOCs are found at the end of Section 3.
- The Company will want to analyze the CSOCs for:
  - **Relevancy:** determine whether the individual CSOC is applicable to the Company's environment. If not, provide details on why it is not applicable.
  - **Control Mapping:** if a CSOC is applicable, the Company will need to obtain the carved-out subservice organization's SOC report. An analysis will need to be performed on that SOC report focused on the specific CSOCs identified in the original report.
  - **Example CSOCs:** data center hosting (AWS, Azure, etc.) tends to be the most common type of service carved-out of original reports.

SECTION 3

# Example CSOCs

## Complementary Subservice Organization Controls (CSOCs)

ABC's controls relating to its security management and support services system cover only a portion of the overall internal control for each user entity of ABC. It is not feasible for the control objectives relating to the security management and support services system to be solely achieved by ABC. Certain control objectives specified in the description can be achieved only if CSOCs contemplated in the design of ABC's controls are suitably designed and operating effectively, along with controls at ABC. Therefore, each user entity's internal control over financial reporting should be evaluated in conjunction with ABC's controls, taking into account the related CSOCs expected to be implemented and operating effectively at the subservice organizations, as described below.

| Number | CSOCs | Applicable Control Objective |
|---|---|---|
| *[Subservice Organization #1 name]* | | |
| 1. | IT general controls, including controls around change management, logical security, physical security, infrastructure, and IT operations, are implemented and effective. | CO6, CO9 and CO12 |
| *[Subservice Organization #2]* | | |
| 2. | Security transactions are processed accurately and timely. | CO3 |
| 3. | Proxy voting processing and reporting is complete, accurate, and in accordance with instructions from ABC. | CO8 |
| 4. | IT general controls, including controls around change management, logical security, physical security, infrastructure, and IT operations, are implemented and effective. | CO6, CO9 and CO12 |

SECTION 4

# Results of Tests of Operating Effectiveness

- The fourth section of each SOC report is the detailed testing results provided by the Service Auditor.
- This section provides testing results of each of the in-scope controls and any deviations identified in the corresponding testing.
- The Company will want to analyze the testing results for:
  - **Approach and Attributes:** ensure the Service Provider took a reasonable approach to each control test and certain aspects of the control were not overlooked.
  - **Testing Results:** determine if there were any deviations identified as a result of the Service Auditor's testing. If deviations were identified, the Company will need to determine if the deviations impact the Company's control environment. Such deviations should be treated as any other deviation identified during the course of the audit would be treated. Additionally, the Service Provider may have included a "Management Response" to the deviation. This response can be used to support mitigation of the deviation if the service auditor performs additional procedures to validate the response.

SECTION 4

# Results of Tests of Operating Effectiveness: Example

| **Control Objective 7:** | | |
|---|---|---|
| **Controls provide reasonable assurance logical access to system resources is restricted to properly authorized individuals.** | | |
| *Description of Controls Provided by ABC* | *Tests Performed by XYZ LLP* | *Results of Tests* |
| 7.2 - Selected IT Analysts are responsible for creating and modifying access profiles to the xxx application. The IT manager manages the user rights of the Analysts IDs. In addition, a weekly review is performed of IT Analyst activity. | Inspected a listing of xxx users to determine whether administrative access was appropriately restricted to selected IT Analysts and the IT manager. | Deviation noted.<br><br>XYZ noted that a user wo transferred from IT to HR on 4/14/20xx still had an active application-level administrative account.<br>Per inspection of the AD domain user listing, we verified that the admin account for the noted user was disabled on 4/28/20xx. We further noted that the last login was on 4/25/20xx. Furthermore, we also obtained evidence from xxx showing the account was disabled at the application level on 9/29/20xx. |
| 7.3 - ABC security policies, standards and procedures govern security to ABC systems. The policies are reviewed and updates as need, but at least annually. | Inspected the ABC IT policy regarding security to determine whether the policy outlined security requirements.<br><br>Inspected the ABC IT policy to determine whether it was reviewed at least annually. | No deviations noted.<br><br>No deviations noted. |
| *7.2 Management response:*<br>*To ensure that IT admin accounts are disabled when an employee terminates or changes job titles, we are creating a User Creation Template for IT staff changes and disables. This template will add a new asset to the ticket to IT admin account review. In order for a user setup ticket to be completed, it must be determined if the staff member has an admin account and if it should be disabled or left active. These new controls will make sure that the admin accounts are disabled when appropriate because of a job change or termination.* | | |

SECTION 5

# Additional Information Provided by Management

- The fifth section of each SOC report is an optional section that will not be seen in every report. This section includes additional information the Service Provider wished to share with the readers of the report. It may include background on the scope and services. It often includes context/responses to any deviations identified in Section 4.
- It is important to remember that **everything is Section 5** is unaudited. Section 5 is wholly owned by the Service Provider and the Service Auditor has no influence on the section and they do not audit any of the responses in this section made by the Service Provider. As such, any “Management Responses” to deviations found in Section 5 cannot be used as mitigation for deviations identified in Section 4.

# Final Thoughts and Takeaways

**Background:** SOC reports provide valuable insights into the controls and processes of service organizations. There are various types of SOC reports and focus areas.

**Benefits:** SOC reports can be a valuable tool for vendor risk management. They play an important role for ongoing compliance and continuous improvement.

**Assessments:** Users of a report should determine its reliability and relevance and the different sections of a SOC report, including the control objectives, testing procedures, and results

2023 INTERNAL AUDIT WEBINAR SERIES

# Questions?

# Thank You


## JAMEY LOUPE

Managing Director
Data Risk & Controls
Risk Advisory Services

jloupe@bdo.com



## MATT BEHAN

Director
Data Risk & Controls
Risk Advisory Services

mbehan@bdo.com

Now
Available
for Download

Join Us for Additional Events in the 2023 Series!

# Upcoming Event

**About BDO USA**

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C, a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

**www.bdo.com**

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.