ISSUE
02
2013

The Auditor's Report

We are starting a new "Reader Section" in *The Auditor's Report* newsletter and we need your help. We want to know what topics YOU are interested in. Send us your topic ideas and/or questions and we will include them in our newsletters. Email us today at news@nearman.com.

In this issue

A PUBLICATION OF
Nearman Maynard • Vallez
Certified Public Accountants

Service Organization Control Reports

Why are Service Organization Control (SOC) reports important to credit unions? The use of SOC reports can be a vital means to provide assurance and trust of the controls of the service organizations used by credit unions. As outsourcing and cloud computing become more widespread and continue to evolve, there is even greater concern about how these processes are being performed by third party service providers. In 2010, the American Institute of CPAs (AICPA) issued new auditing standards and guides for Service Organization Control (SOC) reports to replace the antiquated SAS 70 standards and audit guide. The new standards for SOC reports became effective on June 15, 2011 and were incepted as a means of moving towards more globally accepted international standards. SOC reports not only build on the former SAS 70 reports, they also provide more reporting options to address non-financial transactions and assurance needs. Let us look at the different types of SOC reports and their uses:

SOC 1 reports are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. Under SSAE16, SOC 1 reports retain the original purpose of SAS 70 reports by providing a means of reporting on the system of internal control and processes for complying with internal control for *financial reporting purposes*. While the SAS 70 audit standard required a description of the *controls* of a service provider, SSAE 16 expands this to require a description of the *system* which is supposed to be more comprehensive than the controls description. SSAE 16 requires a written statement of attestation by the management of the service organization. This is supposed to give additional assurance to credit unions because the service provider's management has to issue specific clauses in the report about their system that they attest to.

There are two types of reports for SSAE 16 SOC 1 reports which are similar to the former SAS 70 reports:

> ***"Credit unions should be reviewing the controls of their service providers."***

- Type 1 reports on management's description of the service organization's system and the *suitability of the design of controls* to achieve the control objectives included in the description.
- Type 2 reports are similar to type 1 reports but goes further by also looking at the *effectiveness* of the controls included in the description *throughout a specified period.*

Keep in mind SSAE 16 SOC 1 reports provide assurance by establishing credibility and trust of the service provider's controls and is limited to controls related to *financial reporting*. These reports are intended for existing user entities and their auditors. Credit unions may also want to look at the other SOC reports.

SOC 2 reports are intended for the management of service organizations as well as stakeholders. SOC 2 reports are based on Attestation Standards, Section 101 of the AICPA Codification Standards (AT 101), using criteria in TSP section 100. SOC 2 reports provide assurance about a service organization's information systems controls pertaining to its security, availability, processing integrity, confidentiality or privacy.

There are also two types of SOC 2 reports: both types report on management's description of the service organization's system and the suitability of the controls design. A type 2 SOC 2 report goes further by addressing the operating effectiveness of the controls.

SOC 3 reports are similar to SOC 2 reports and are based on AT 101, Attestation Engagements, using predefined criteria in TSP 100. SOC 3 reports are intended for the general public and may address system controls for all areas mentioned for SOC 2 reports. However, SOC 3 reports do not require a detailed description of controls related to compliance or operations or detailed testing procedures and the results of these tests. SOC 3 reports generally provide a higher level of assurance to the public whereas SOC 2 reports are usually restricted to use by the service provider's management and clients.

SOC reports help management to understand the risks of outsourcing to service providers. SOC reports provide assurance on the controls of credit union service providers relevant to:

- The financial reporting of the service organization (SOC 1 report)
- Specified compliance or operations areas (SOC 2 & 3 reports)

Credit unions should be reviewing the controls of their service providers. As the urgency for better protection and security of data grows, credit unions and their auditors need to understand and have confidence in the controls in place of its service providers. A great way to achieve this is by examining the SOC reports for these service organizations.

Nicole Lee, MPA, Audit Manager
Nearman, Maynard, Vallez, CPAs

Auditing the Area of Cash

The area of cash and cash equivalents is usually considered a risk area that requires good internal controls and careful monitoring. This article outlines the testing that supervisory/audit committees, risk management departments, and internal audit departments may want to consider as part of their review of the internal controls in the area of cash and cash equivalents.

Conduct surprise cash and cash equivalent counts. Cash counts should be conducted throughout the year and should cover all branches and, if possible, all tellers. Cash counts could be on a "spot basis" and may cover all and/or a sample of tellers. In addition, other cash and cash equivalent areas should be covered in these counts which include, but are not limited to, cashier checks, travelers' checks, money orders, movie tickets, stamps, etc.

Also, check the teller drawers to determine if tellers have any of their own personal checks in his/her cash drawer. It is not uncommon for tellers to place their personal checks in their drawer without "dating" the check. The embezzlement of funds is accomplished by the teller taking money for long periods of time and in the event of a surprise cash count, the teller states that the check was placed into the drawer that day and that he/she forgot to date the check.

Bait money. Bait money are bills whose serial numbers are recorded in a log book. During a bank robbery, if the robber has taken the bait money, details can be passed onto the police. If the money is in the possession of someone or used to purchase goods then it is often easier to identify the perpetrator of the bank robbery. Not having bait money could make it difficult to trace these funds in the event of a robbery. Since the majority of the cash on hand is maintained in the vault, it is also recommended the vault be assigned bait money.

Care should be taken if bait money is photocopied. The law strictly restricts photographs or other printed reproductions of paper currency. Black and white reproductions are permissible but must be larger than one and one-half times (150%) or smaller than three-quarters of the size (75%) of the genuine. Photocopies and/or the bait money control log should be maintained in a secured location, preferably away from the cash area.

During cash counts, the bait money should be verified to the bait money control list. Lastly, bait money should be periodically rotated to ensure the bait money does not give the appearance of being old.

Test dual custody or dual control procedures. Dual custody requires that a minimum of two people are required to physically access certain items or records and are equally accountable for their protection. For example, one employee has the key and a second employee has the combination to access the ATM machine. Dual control extends that concept by requiring that the work of one employee is verified or approved by a second employee. One employee counts and records the deposits obtained from the night deposit box, a second employee verifies that count. Examples include but are not limited to:

- Reserve cash, negotiable instruments, unissued traveler's checks, the night depository, the vault, ATM machines, the reserve supply of official checks; are examples of items and areas that should be under dual custody. Walk through the steps to obtain these items or access these areas to ensure at least two people are required to obtain access.
- Night depository procedures should be done under dual control. For example; withdrawal of funds, opening of bags, recording of bag numbers, envelope numbers, and depositors' names, and counting and verifying the contents of the envelopes. Review a sample of daily work for dual control sign off.
- Deposits received by mail should be opened under dual control. Review a sample of daily work for dual control sign off.
- Logs should record entrance and exits to the vault, ATM machines, night depository, safe deposit boxes, etc. Review logs for completeness and appropriate access granted.
- Currency shipment procedures (sending and receiving) should be done under dual control. Verify procedures with appropriate personnel and review cash order receipts for appropriate signatures.

Review mandatory vacation policies. The credit union should have a written vacation policy that mandates employees be absent from their duties for an uninterrupted period of not less than one week. In an employee's absence, someone else should assume their duties as a fraud prevention/detection tool. To ensure the policy is enforced, select a sample of employees and verify the mandatory vacation was taken in the prior year.

Review teller cash overage/short accounts. There should be written procedures in place for prompt reporting and investigating of shortages when they become known. Cash overages/shortages should be properly recorded in a cash over/short account. Review account details for recurring patterns or any large or unusual items. Ensure shortages have been properly investigated and resolved.

Test key and combination assignments. The credit union should have a record of all keys and combinations issued to employees. Physically verify each employee has in his or her possession the keys assigned from this record and these keys are secured and not located in an unlocked drawer or file cabinet. Keys should be retrieved and combinations changed when an employee terminates. Review records to ensure this has occurred if an employee with possession of a key or combination has recently terminated. Unassigned keys should be kept under dual control. Walk through the steps to observe how access to these keys is obtained to ensure at least two people are required to gain access to the keys.

Review of other procedures and controls. Your credit union may have other controls in place for security of cash and the teller function. Does credit union's policy and procedures require any of the following? If yes, verify practice is consistent with written policy.

- ***Pocketless uniforms or clothing for tellers***. Several credit unions have required that tellers wear uniforms which are pocketless. However, the implementation of this requirement would be based on a cost versus benefit basis depending on each credit union.
- ***Receipts for all transactions***. Management should consider making it a requirement that tellers provide each member with a receipt reflecting the member's transaction. Each teller station should have a sign posted that states:

Continued on next page

Nearman Maynard•Vallez
Certified Public Accountants

About Us

Since 1979, Nearman, Maynard, Vallez, CPAs has provided auditing and consulting services exclusively to credit unions throughout the United States. Our dedication to credit unions has given us the unique ability to provide exceptional service at a reasonable price. Our primary objective is to assist our clients in accomplishing their goals through our experience, service, & commitment. If your Supervisory/ Audit Committee or Management is interested in obtaining information on the subjects in this issue or about our many services, call or email us today.

Website:
www.nearman.com
E-mail: info@nearman.com
Toll-free: 800.288.0293

Atlanta: 205 Brandywine Blvd., Suite 100,
Fayetteville, GA 30214
770.461.5706
770.719.1888 fax

Miami: 10621 N. Kendall Dr., Suite 219,
Miami, FL 33176
305.598.1730
305.595.9316 fax

Continued from previous page

> *"All members must be provided with a printed receipt as part of your transaction. In the event that the member does not receive a receipt, please notify Management."*

- ***Installation of video cameras***. Video cameras should be placed in strategic places where there are cash and cash equivalents. In addition, while most video cameras are installed to monitor member activity, consideration should be considered in areas behind the teller lines and in areas where there is continuous traffic. Also, if the tellers have an area where they store their personal belongings during the working hours, the installation of a video camera in this area should be considered.
- ***Lockers installed outside the cash area***. The credit union may want to establish an area outside of the teller area where credit union employees can place their personal belongings away from the area where cash and cash equivalents are maintained. This procedure could prevent the transfer of unauthorized funds into the credit union employee's personal belongings.

Review of teller access and authentication mechanisms on the computer system. Access and authentication mechanisms on the computer system are important tools to ensure accountability and prevent unauthorized access to transactions and information. Review authentication and password policies for appropriateness. Select a sample of employees and review their access rights on the system. Compare system user ID lists to a current employee list from Human Resources to ensure terminated employees have been removed from the system.

- Computer systems require passwords to access the system and should be changed on a frequent basis. We recommend passwords be changed every 45-60 days. In addition, the employees should not be allowed to use the same password.
- Password construction should mandate that passwords be a minimum of six alphanumeric characters and should not be easily guessed. Guidance should be provided about the importance of keeping an employee's password confidential (e.g. not writing it down or sharing it with other employees).
- Computer systems should log out the teller when there has not been activity for a certain period of time (usually 10 minutes). If automatic log-off is not an option, consider screen savers that would activate after 10 minutes of inactivity requiring re-entering the teller's password when returning to the application.
- Terminated employees should be removed from the system as soon as possible to prevent anyone from using that ID for unauthorized access to transactions and information.
- One last point is that tellers should not be permitted to make any transactions to their personal or relative's accounts. It has been noted that tellers who have embezzled in the past have used their relative's accounts for unauthorized activity (Sometimes with and without their relative's knowledge). In addition, teller access to the system should be based on the principle of "least privilege" - limited to those functions required for their job responsibilities.

Policies, procedures, and zero tolerance of fraud. Credit union employees should be informed of the policies and procedures covering the area in which they are working. The credit union's employees should also be informed that the credit union has zero tolerance for any fraud and they will prosecute any credit union representative who violates these policies. In addition, it should also be communicated to all employees that any credit union representative who is aware of a potential fraud has a duty to report this to the appropriate individuals at the credit union. Not reporting this to the appropriate individuals constitutes a violation of the credit union's policies and procedures and the employee will be subject to the same disciplinary actions which will take place against the original abuser. Review the credit union's written policies related to fraud. Determine how these policies are communicated to the employee. If the employee is required to sign an acknowledgment of receiving the policy, select a sample of employees and verify an acknowledgment was signed.

Based on the information presented in this article and the potential for detecting fraudulent activity, we strongly recommend that credit unions consider the recommendations we have discussed. Most of the items are proactive measures and a psychological deterrent, which should aid the credit union in their monitoring of these sensitive areas.

Cecil D. Maynard, CPA, MPA, CFE, CFF, Partner
Nearman, Maynard, Vallez, CPAs, P.A.

Associate Spotlight

Nearman, Maynard, Vallez is proud to announce that **Tammy Fletcher, Internal Audit Manager**, has successfully attained the certification of NAFCU Certified Compliance Officer (NCCO). To become certified, Tammy passed a series of four examinations which cover a wide variety of compliance topics. By obtaining the NCCO designation Tammy has shown she has a comprehensive understanding of the major regulations that govern credit union operations.

Congratulations Tammy!