DCU BULLETIN

Division of Credit Unions

Washington State Department of Financial Institutions

Phone: (360) 902-8701 ***FAX: (360) 704-6901***

March 25, 2008 No. B-08-03

Management of Third Party IT Service Providers

Credit unions rely on external service providers for a variety of services. Division Information Technology (IT) examiners continue to cite credit unions for incomplete vendor management programs. This bulletin should assist credit unions in performing better service provider oversight. This guidance provides the key elements in reviewing a service provider's SAS 70 audit report and provides the main elements of contract language relating to the security and privacy of member information. Other important contract provision areas including, but not limited to, the rights and responsibilities of both parties, adequate and measurable service level agreements, are not discussed in this bulletin. Suitable documentation should be in place at the credit union to demonstrate a thorough review of SAS 70 audit reports and vendor contracts.

Credit unions need to be assured that their service providers have implemented appropriate controls over the credit union's business processes and information technology. This is especially important for vendors with access to member information. Examples of such vendors are the core banking system provider and the statement printing vendor.

SAS 70 Audit Reports

Examiners will expect credit unions to review each vendor's SAS 70 audit report and document the results of that review.

What is a SAS 70 audit report?

A SAS 70 audit is the standard used by vendors to demonstrate the existence and effectiveness of their internal controls. SAS 70 audits, also referred to as a service auditor's report, come in two types. A SAS 70 Type I audit is an audit engagement that reviews the effectiveness of an organization's internal control descriptions (policies and procedures) based on the AICPA Statement of Accounting Standards No. 70. Type II audits actually test the controls over some period of time.

The Type I SAS 70 audit includes the vendor's description of its controls and objectives, and the auditor's opinion on the suitable design of these controls in meeting the specified objectives.

The Type I report reflects an opinion at a specified point in time.

The Type II SAS 70 report, in addition to the Type I components, includes the auditor's comments after testing the effectiveness of the internal controls. The Type II report attests to the effectiveness of the controls in meeting the specified objectives over a period of time, typically six months.

A Type II SAS 70 audit is more desirable (and more expensive) than a Type I audit because testing was performed on the effectiveness of the internal controls. If a credit union receives a Type I SAS 70 audit and report, it should consider obtaining additional assurance regarding the effectiveness of the service provider's internal controls.

Benefits of a Vendor's SAS 70 Certification

A vendor's unqualified SAS 70 opinion provides the following:

- Insight into the nature of a vendor's controls and an independent party's assessment of their effectiveness;
- A reasonable assurance that the vendor has established internal controls that are operating effectively; and
- It eliminates the burden and cost of a credit union having to perform a separate audit of a vendor.

SAS 70 Audit Report Review Process

A credit union should formally document its review of each vendor's SAS 70 report by completing the steps outlined below.

1) Verify the applicability of the SAS 70 audit to the services the vendor provides to the credit union. The SAS 70 audit should address the services used by the credit union. For example, if the credit union uses a vendor's online banking service, the SAS 70 audit report must address this service.

2) The SAS 70 audit date – It is important to verify whether the SAS 70 audit is current. Look for the date or date range that the controls were evaluated. This is also an easy way to determine if you are looking at a Type I or Type II report. Type I audits are usually for a point in time, whereas Type II audits discuss the operating effectiveness of controls over a period of time.

3) Examine the opinion letter - If any weaknesses or deficiencies are identified in the SAS 70 audit report opinions, the credit union must assess the potential impact of these weaknesses or deficiencies and the adequacy of the vendor's resolution plans. The resolution plans are usually detailed within the body of the SAS 70 report. If a Type I SAS 70 audit was performed, the credit union should consider obtaining additional assurances as to whether vendor's internal controls are effective.

4) Client Controls - The SAS 70 audit report should identify client control points for the user's consideration. These are controls that should be in place at the credit union. The

reviewer should ensure these controls are in place or are in the process of being implemented within the credit union.

Vendor Contracts Must Contain Language to Protect Member Information

Credit unions should review contracts with vendors to determine whether the contract contains clauses to protect non-public member information. Contracts with vendors who receive non-public member information should include appropriate language requiring the vendor to implement controls to maintain the confidentiality and security of member information according to the Gramm-Leach Bliley Act (GLBA). In addition NCUA Letter to Credit Unions 07-CU-13 (Evaluating Third Party Relationships) also emphasizes this point. This includes, but is not limited to, notifying the credit union when the vendor suspects or determines that member information has been compromised. It also should include provision for the return or destruction of member information upon contract termination. Some credit unions have found it important to include language that provides for credit union testing of the vendor protection for member information. If necessary, contract amendments should be executed with vendors.

Please contact Glenn Ross at (360) 481-2551 or Doug Lacy-Roberts at (360) 902-0507, if you have any questions.