Alaska Department of Education & Early Development

Dillard Research Associates

Alaska Alternate Assessment

Website Security Assurances

November 2010

ISSUE 1: Secure access and access to http://ak.k12test.com (The test training site was unsecure)

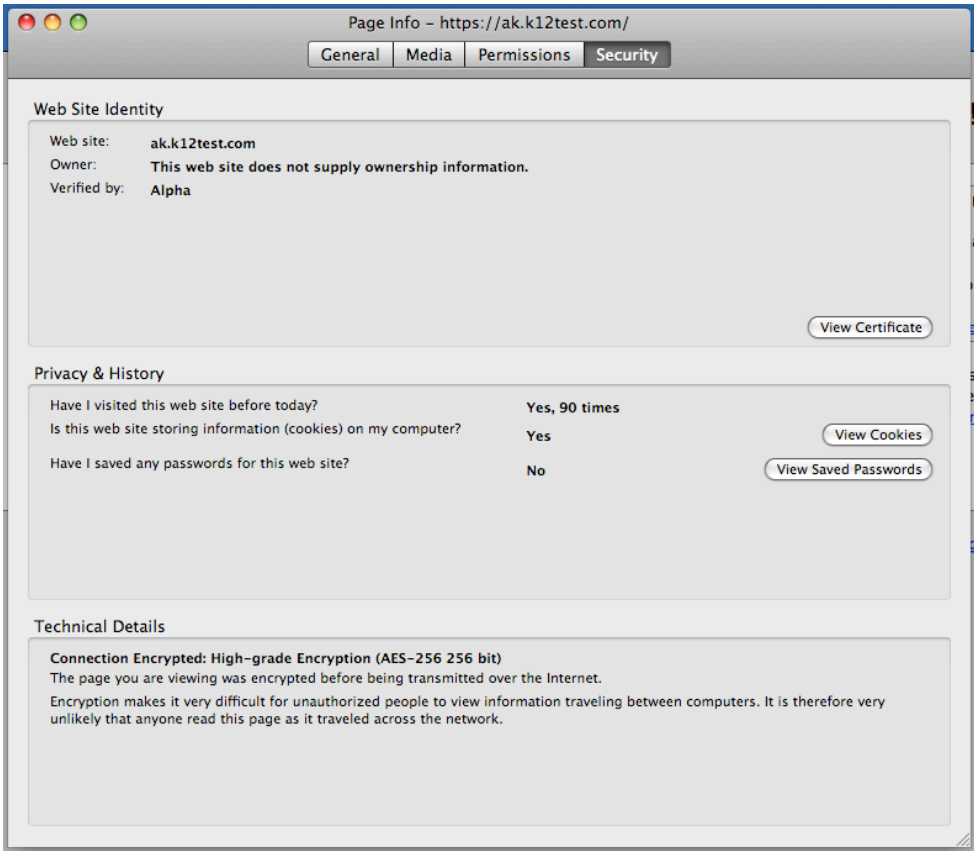
DRA proposed securing the entire website for the entire school year, forcing all districts to address security blocks early in the school year, rather than toward the end of the testing window.

The Site was made secure in August 2010.

In September, 2010, Kim Sherman asked the programmers to remove the security shield from the site to prevent access issues occurring during New Mentor and Annual Mentor Trainings. Kim neglected to request that the security shield be reinstated at the conclusion of Annual Mentor Training.

The security for the entire system has been re-established. No security breach transpired, as no confidential student data are available on the site until January 31, 2010.

ISSUE 2: Security of the website, the hosting servers, and transfer of secure data
To secure the AK website, a wildcard SSL certificate was purchased (for several hundred dollars) and installed on the web server. This uses Advanced Encryption Standard (AES) 256-bit high-grade encryption - the same level of encryption used by banks. I've included several attachments which verify and document the security of the website. See below.



Web Site Identity

Web site: ak.k12test.com
Owner: This web site does not supply ownership information.
Verified by: Alpha

Privacy & History

Have I visited this web site before today? Yes, 90 times
Is this web site storing information (cookies) on my computer? Yes
Have I saved any passwords for this web site? No

Technical Details

Connection Encrypted: High-grade Encryption (AES-256 256 bit)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

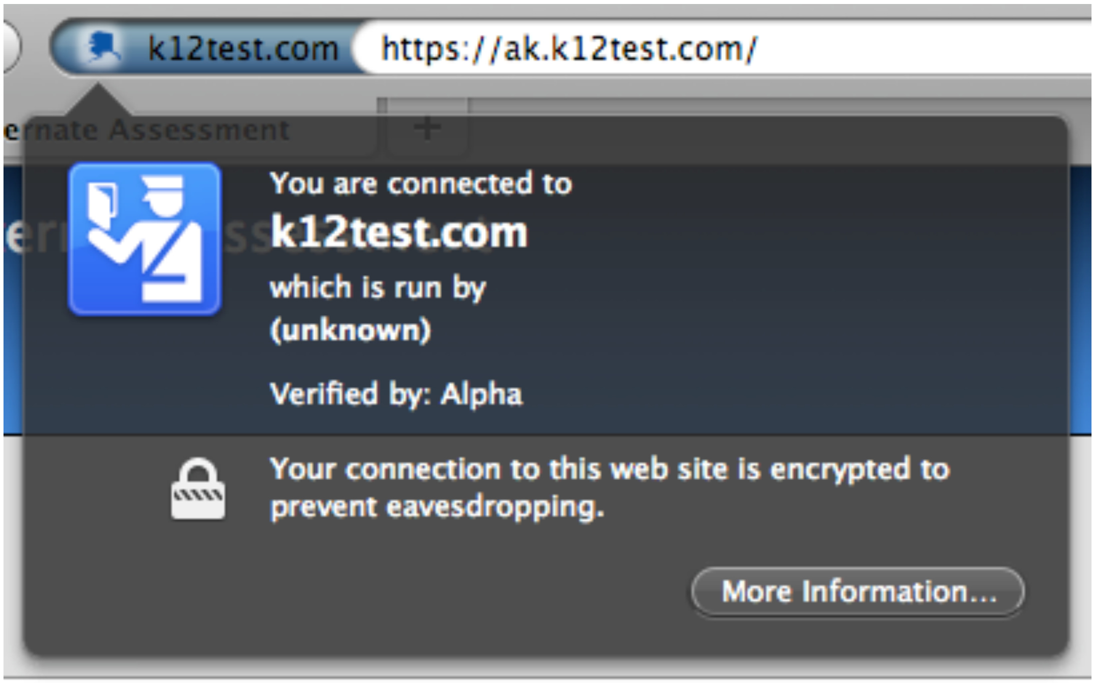
ISSUE 3: Security of the secure transfer site (filetrans.easycbm.com)
The AK website makes use of the cryptographic protocols Transport Layer Security (TSL) and Secure Socket Layer (SSL) to provide security from each end user's computer and the website's server. In order for this to work, a public key certificate has to be installed on the web server and signed by a trusted Certificate Authority (such as VeriSign or Alpha). Web browsers connect to the website over HTTPS using port 443, and after a series of handshakes using public and private keys, a secure connection is established. Basically any information sent from the website to a users computer, and vice versa, is encrypted before being sent. This ensures protection from eavesdroppers and man-in-the-middle type attacks.

The Secure File Transfer Protocol (SFTP) server used for AK files (the "Fetch Server") uses a very similar technology, though it encrypts connections over port 22 instead of 443. Web servers can be configured to simultaneously listen for requests over the http:// protocol on port 80 as well as the https:// protocol on port 443, for increased compatibility with browsers, computers, and network settings. Based on previous feedback, the AK website was recently configured in this fashion to ensure successful mentor trainings, such as the one that took place last week, so that computer settings and network filters/configurations would not hamper the trainings. As these trainings have concluded, the web server has been configured to force all web traffic requests to come over HTTPS.

FTP servers such as our "Fetch Server" don't use http or https, but rather ftp and sftp instead. These are similar concepts, but different protocols and port numbers. Looking at Aran’s copy/paste, it appears that she's using the File Zilla client, and the "Response: fzSftp" bit is showing that file zilla is using the Sftp protocol to connect. You can also see that 'open "akdoe@filetrans.easycbm.com" 22' is using port 22 (the standard port for SFTP), rather than port 21 (the port for plain FTP).

The AK website and SFTP server are located in Seattle, Washington and hosted with the highly reputable company SoftLayer. SoftLayer’s hosting services are certified reliable and secure, having received Statement on Auditing Standards No. 70 (SAS 70) Type II Certification. This includes a full assessment of: Oversight by Executive Management, Operations and Customer Service, Development and Information Technology Organization, Human Resources Policies and Procedures, and Risk Assessment Monitoring. Such a review is important for service organizations, such as DRA, that provide services that are critical to its customers’ operations - the SAS 70 Type II Certification provides third-party verification that, in turn, the organization’s customers can supply for audits of their own operations (the audit meets Sarbanes-Oxley requirements). Attached are two PDF documents which go into more detail about SoftLayer's SAS 70 compliance. The server itself uses redundant drives in a RAID configuration, takes nightly backups of the database, and we keep offsite backups as well.

Firefox Reporting the encrypted connection:



You are connected to

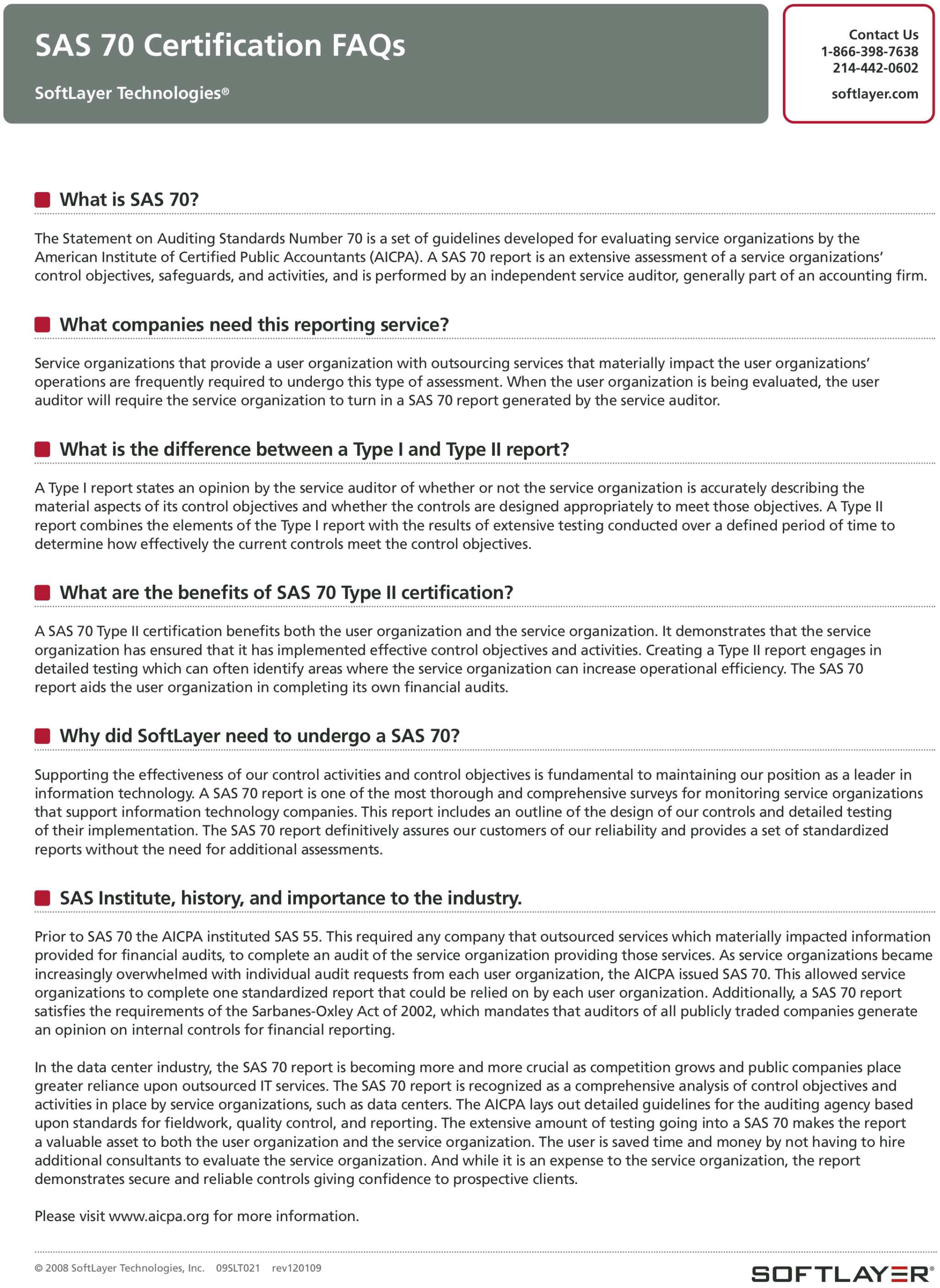
k12test.com

which is run by
(unknown)

Verified by: Alpha

Your connection to this web site is encrypted to prevent eavesdropping.

Certificate Verification and Technical Details:



SAS 70 Certification FAQs

SoftLayer Technologies®

Contact Us
1-866-398-7638
214-442-0602

softlayer.com

What is SAS 70?

The Statement on Auditing Standards Number 70 is a set of guidelines developed for evaluating service organizations by the American Institute of Certified Public Accountants (AICPA). A SAS 70 report is an extensive assessment of a service organizations' control objectives, safeguards, and activities, and is performed by an independent service auditor, generally part of an accounting firm.

What companies need this reporting service?

Service organizations that provide a user organization with outsourcing services that materially impact the user organizations' operations are frequently required to undergo this type of assessment. When the user organization is being evaluated, the user auditor will require the service organization to turn in a SAS 70 report generated by the service auditor.

What is the difference between a Type I and Type II report?

A Type I report states an opinion by the service auditor of whether or not the service organization is accurately describing the material aspects of its control objectives and whether the controls are designed appropriately to meet those objectives. A Type II report combines the elements of the Type I report with the results of extensive testing conducted over a defined period of time to determine how effectively the current controls meet the control objectives.

What are the benefits of SAS 70 Type II certification?

A SAS 70 Type II certification benefits both the user organization and the service organization. It demonstrates that the service organization has ensured that it has implemented effective control objectives and activities. Creating a Type II report engages in detailed testing which can often identify areas where the service organization can increase operational efficiency. The SAS 70 report aids the user organization in completing its own financial audits.

Why did SoftLayer need to undergo a SAS 70?

Supporting the effectiveness of our control activities and control objectives is fundamental to maintaining our position as a leader in information technology. A SAS 70 report is one of the most thorough and comprehensive surveys for monitoring service organizations that support information technology companies. This report includes an outline of the design of our controls and detailed testing of their implementation. The SAS 70 report definitively assures our customers of our reliability and provides a set of standardized reports without the need for additional assessments.

SAS Institute, history, and importance to the industry.

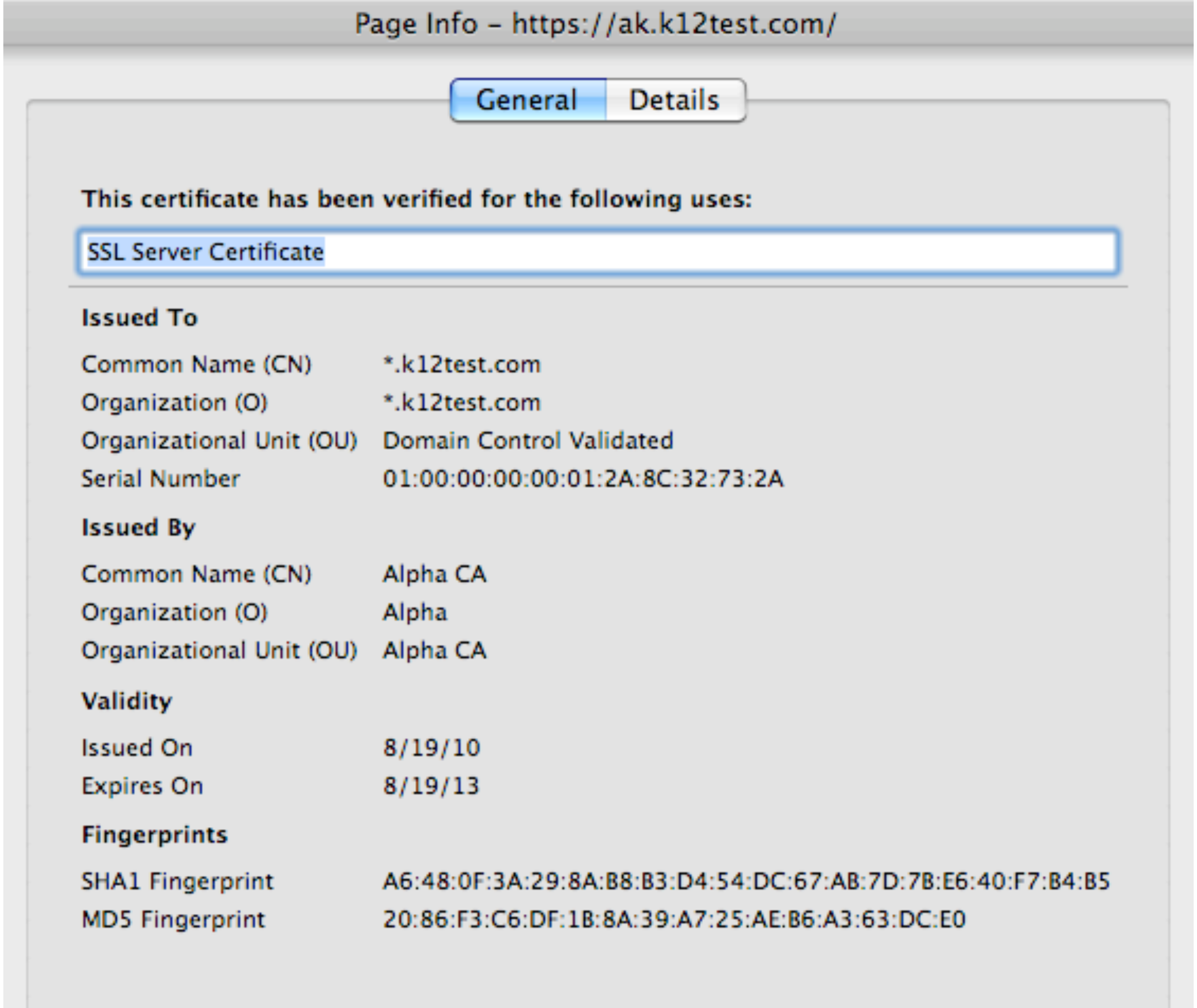
Prior to SAS 70 the AICPA instituted SAS 55. This required any company that outsourced services which materially impacted information provided for financial audits, to complete an audit of the service organization providing those services. As service organizations became increasingly overwhelmed with individual audit requests from each user organization, the AICPA issued SAS 70. This allowed service organizations to complete one standardized report that could be relied on by each user organization. Additionally, a SAS 70 report satisfies the requirements of the Sarbanes-Oxley Act of 2002, which mandates that auditors of all publicly traded companies generate an opinion on internal controls for financial reporting.

In the data center industry, the SAS 70 report is becoming more and more crucial as competition grows and public companies place greater reliance upon outsourced IT services. The SAS 70 report is recognized as a comprehensive analysis of control objectives and activities in place by service organizations, such as data centers. The AICPA lays out detailed guidelines for the auditing agency based upon standards for fieldwork, quality control, and reporting. The extensive amount of testing going into a SAS 70 makes the report a valuable asset to both the user organization and the service organization. The user is saved time and money by not having to hire additional consultants to evaluate the service organization. And while it is an expense to the service organization, the report demonstrates secure and reliable controls giving confidence to prospective clients.

Please visit www.aicpa.org for more information.

SOFTLAYER®

SSL Server Certificate with SHA1 and MD5 fingerprints:



Page Info – https://ak.k12test.com/

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	*.k12test.com
Organization (O)	*.k12test.com
Organizational Unit (OU)	Domain Control Validated
Serial Number	01:00:00:00:00:01:2A:8C:32:73:2A

Issued By

Common Name (CN)	Alpha CA
Organization (O)	Alpha
Organizational Unit (OU)	Alpha CA

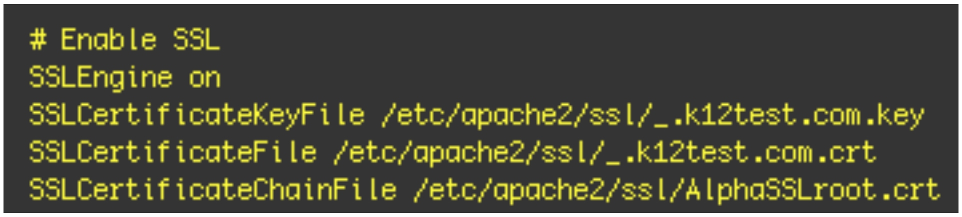
Validity

Issued On	8/19/10
Expires On	8/19/13

Fingerprints

SHA1 Fingerprint	A6:48:0F:3A:29:8A:B8:B3:D4:54:DC:67:AB:7D:7B:E6:40:F7:B4:B5
MD5 Fingerprint	20:86:F3:C6:DF:1B:8A:39:A7:25:AE:B6:A3:63:DC:E0

Apache Directives enabling SSL on the server:



```
# Enable SSL
SSLEngine on
SSLCertificateKeyFile /etc/apache2/ssl/_.k12test.com.key
SSLCertificateFile /etc/apache2/ssl/_.k12test.com.crt
SSLCertificateChainFile /etc/apache2/ssl/AlphaSSLroot.crt
```

SoftLayer SAS 70 compliance additional documents:

BKD LLP
CPAs & Advisors

One Metropolitan Square
211 N Broadway, Suite 600
St. Louis, MO 63102·2733

Board of Directors
SoftLayer Technologies, Inc.
Dallas, Texas

Independent Service Auditors' Report

We have examined the accompanying description of controls provided by SoftLayer Technologies, Inc. relative to its order processing operations, including the general and certain OTRS application controls related to the Dallas, Seattle and Washington D.C. Data Centers. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of SoftLayer Technologies, Inc. 's controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of SoftLayer Technologies, Inc.'s controls; and (3) such controls had been placed in operation as of October 31, 2009. SoftLayer Technologies, Inc. uses ViaWest, Sabey and 356 Main for hosting of the physical servers and devices used by SoftLayer Technologies, Inc. The accompanying description includes only those control objectives and related controls of SoftLayer Technologies, Inc. and does not include control objectives and related controls of ViaWest, Sabey and 356 Main. Our examination did not extend to controls of ViaWest, Sabey and 356 Main. The control objectives were specified by the management of SoftLayer Technologies, Inc. Our examination was performed in accordance with the standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the SoftLayer Technologies, Inc. controls presents fairly, in all material respects, the relevant aspects of SoftLayer Technologies, Inc.'s controls that had been placed in operation as of October 31, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of SoftLayer Technologies, Inc.'s controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls listed in Section III of this report, to obtain evidence about their effectiveness in meeting the related control objectives, described in the Control Objectives Matrices of Section III, during the period from November 1, 2008 to October 31, 2009. The specific controls and the nature, timing, extent and results of the tests are listed in the Control Objective Matrices of Section III. This information has been provided to user organizations of SoftLayer Technologies, Inc. and to their auditors to be taken into consideration, along with the information about the internal control of user organizations, when making assessments of control risk for user organizations. In our opinion, the controls that were tested as described in the Control Objective Matrices of Section III, were operating with sufficient effectiveness to provide