

Welcome to *Policy Matters*, an engaging and informative monthly e-newsletter featuring expert insight and analysis on emerging relocation products, policies and services that can provide immediate benefit to your organization.

Anatomy of a SAS 70 Report: One Method of Ensuring Data Safety and Security

Data has become the currency of our economy. As a result, companies spend a significant amount of money, time and resources to ensure that their data – and the data of their employees – is safe and secure.

This task is becoming increasingly challenging as a number of organizations are outsourcing non-core elements of their business to third-party organizations. Data is being shared and, in some cases, controlled by other companies. Additionally, the ever-changing legal landscape at the local, state, federal and international level requires companies to ensure that data—especially personally identifiable information—is safe and secure.

In discussing data security, it is important to understand the states of data and how they relate to the various control considerations within one of these audits.

The three states of data are:

- 1) **Data at rest** refers to any media that stores data, including server hard drives, tapes, and other media
- 2) **Data in motion** is the state where data is being transmitted from one location to another. Examples include e-mail transmissions, file downloads from an FTP (file transfer protocol) site, and business-to-business integrations such as integrated web services
- 3) **Data in use** refers to the line of business applications that access data in order to deliver service or process information such as a Human Resource Information System (HRIS) or other financial platforms

Companies must work to ensure that information leaving the premises and going to an off-site provider has the appropriate controls in place to protect the data. But while a third-party organization may provide every assurance that their data is safe, how can a company really know that the data they provide to a service organization is secure?

One possible solution, of many, is SAS 70. SAS 70's full name is the Statement on Auditing Standards No. 70: Service Organizations, and it is an auditing standard developed by Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). Quite simply,

SAS 70 ensures that a third-party organization has controls and processes in place to ensure that data is secure and that appropriate financial controls protect the company.

SIRVA has conducted annual SAS 70 audits since 2004 to demonstrate its commitment to securing customer data. SAS 70 is specifically designed for service organizations, and the audit covers a service organization's comprehensive data-protection environment—from the computing operation, physical and logical security to the business processes.

In this Issue of *Policy Matters*, we'll explore why it is vital to ensure you are working with an organization who has conducted a thorough SAS 70 audit, how an audit is constructed, and how to identify what elements are core to a comprehensive SAS 70 audit.

Ensuring Compliance

The report resulting from a SAS 70 audit provides a customer the assurance that the third party with whom they are working has the right financial controls and data protection in place.

Any customer looking to partner with a service organization—like a relocation provider—should understand the importance of having some kind of independent affirmation of the service provider's data and financial protection.

It comes down to the difference between having a service organization essentially say “trust us, we've got the proper controls and procedures in place” to having a third party, independent auditor say, “yes, we've inspected the service organization's operations, and have verified that all the controls are in place—and your data is secure.”

The Anatomy of a SAS 70 Report

The first step in preparing a SAS 70 report is determining what criteria, controls and processes will be tested. The service organization being audited will review the guidelines established by the AICPA to determine what controls to include in the audit. This information is then included in the service organization's description of controls at the beginning of the report.

As part of this initial scope of the report, the service organization can provide background on its user control considerations, which provides details on the applications where clients can set up their own users.

As a result of the criteria and user control considerations, no two SAS 70 reports are the same, as the service organizations make the determination of what controls will be evaluated specific to the company's processes and operating procedures. However, there are some baselines in each one of the report sections that must be included in order to provide reasonable assurance that data is secure at rest, in motion, and in use.

During the evaluation period, the service organization can determine if they will participate in a Type I or Type II version of the SAS 70 report. However, a Type 1 report only provides half of the picture, and on its own is not adequate.

In a Type I report, the service organization essentially provides a narrative description of what controls are in place. While this report may contain a listing of the various controls and processes, it doesn't share whether or not those controls and processes have been tested by an independent auditor for effectiveness and results.

That's why a Type II report is a much more comprehensive, verifiable approach to ensuring data security. A Type II report will define all of the controls and processes outlined in the Type I report, but then will verify those controls through tests and note the results and any exceptions.

The tests conducted by the auditor come in three types:

- 1) An inquiry – in this test, a third-party auditor asks the participating service organization questions about the controls they have in place. For example, the auditor may ask about how the company manages its passwords—whether they are at least eight characters in length and contain both alphanumeric and numeric characters.
- 2) An observation – the third-party auditor will watch an IT administrator perform the task being audited. Using the password example, the auditor will watch to see if a password that does not contain the above criteria is rejected by the system.
- 3) An inspection – the third party auditor will go in with the network administrator to verify that the rules created actually work. Again in the password example, the inspection will review all of the passwords to ensure they match the criteria established.

Using these tests, the auditor then provides an opinion on whether the service organization has adequate controls in place. In a SAS 70 report, the auditor will conduct at least two of the three tests on each of the controls to ensure accuracy. In most situations, at least two tests are performed against any single control to ensure that it is functional and valid. For example, the auditor will inquire about the password length from the provider's security manager in conjunction with inspecting the configuration settings for passwords within the administrative console.

If the auditor finds a primary control that is weak or substandard, he or she will then ask the service organization if there is a compensating control to offset it. This becomes important in ensuring who has access to data. For example, an auditor may ask human resources for a current list of employees. The auditor will then compare that list to the registered users in the IT database. If there are users still listed in the database who are no longer employees, then the auditor may indicate that the company has failed in this control. However, the service organization has the opportunity then to present compensating controls. In this example, the company could indicate that it does not immediately remove terminated employees from the database, it simply disables their account. The auditor will then ensure that this compensating control is working.

This same approach works for financial controls. For example, a company may indicate that one of its key financial controls is ensuring that accounts payable doesn't have the authority to establish vendors and approve payments. The auditor may then ask an inquiry about this process, and then inspect to ensure that accounts payable doesn't have this authority.

Once the field period of auditing is complete—that is, that all controls have been tested in two different ways—the auditor then compiles the report in a table format.

In a SAS 70 report, the tables are typically divided into five different domains, which include:

- 1) Control environment, risk assessment and monitoring
- 2) General computer controls
- 3) Logical access
- 4) Systems development and maintenance
- 5) Information systems control

Within each of these domains, a service provider establishes and shares the control objective. An example of a control objective for the first domain (the control environment, risk assessment and monitoring) is:

“Controls provide reasonable assurance that management and the board of directors demonstrate through attitude, awareness and actions an atmosphere that enhances the effectiveness of specific controls.”

The table includes details about what controls are in place to meet the objective, the specifics of the tests conducted, and what the results of the tests were—and in some cases—what compensating controls are in place.

The final element of the report is for the service organization to provide examples of other controls in place. For example, if an organization has a disaster recovery plan or other certifications that would not be covered during the audit, the organization has the ability to add the relevant information to the report.

Locking Up Data Security

In reviewing the elements of a SAS 70 audit, the controls *not* included in the report are of equal importance to those in the report. As is the case with evaluating any type of relationship or business decision, it is important to consider inherent and residual risk. Inherent risk is created from working with a third-party service provider's controls and procedures—and is often the worst case scenario. Residual risk remains after the controls have been instituted to mitigate as much of the inherent risk as possible.

A SAS 70 report is another tool that helps an organization evaluate and understand both types of risks. When companies examine any third-party provider, they should evaluate based on these types of risks and consider the following equation: Risk = Hazard + Outrage. Hazard is the direct cost or harm. Outrage is the public opinion and other opportunity cost. Risk is the total threat to the enterprise and is the sum of Hazard and Outrage.

Protection of critical business and personal information remains paramount in today's data-driven world. As companies continue to partner with new organizations, the data it provides to these organizations must be secured. Companies should review and contact current service providers, whether it is a relocation provider or any third party, to ensure these providers have third-party auditors' opinions confirming the controls and processes in place will protect their data – whether through a SAS 70 or other report. Taking these steps will help companies ensure their data remains secure.

###

Matthew Dickerson is SIRVA's chief innovation officer and is responsible for client-facing technology and innovation projects that serve corporate clients, transferees and moving customers. He is a Six Sigma Green Belt, a certified e-commerce consultant and a certified Internet webmaster associate. As a Certified Relocation Professional (CRP), Dickerson received the Worldwide Employee Relocation Council's (ERC®) 2007 Meritorious Service Award. He holds a B.S. in information systems from Cleveland State University and is currently pursuing graduate studies in information systems.

The foregoing is intended as general information only. SIRVA suggests that decisions as to your specific situation should be made only after full evaluation of your circumstances with your company leadership, tax and legal advisors, and HR personnel.

© 2010 SIRVA, Inc. / www.sirva.com / blog.sirva.com SIRVA and the SIRVA LOGO DESIGN are registered service marks of a subsidiary of SIRVA, Inc.