SAS 70 Type II Audits

Ensuring Data Security, Reliability and Integrity

If your organization shares sensitive data over the Internet, you need rigorous controls to ensure data security, reliability, integrity — as well as regulatory compliance. Those controls must extend to any service organizations to which you outsource, including Software-as-a-Service (SaaS) providers and data hosting facilities.

While you might assume that all service providers offer the same level of protection, security controls vary significantly from one provider to the next. Therefore, you need to ensure that your provider's service is up to appropriate standards to protect your business information. This whitepaper describes how a SAS 70 Type II audit demonstrates the existence and the effectiveness of internal security controls at service organizations, and how IntraLinks meets these standards to provide the highest level of security to our customers.

INTRALINKS®

1 866 INTRALINKS

New York + 1 212 342 7684
London + 44 (0) 20 7549 5200
Hong Kong + 852 3101 7022

www.intralinks.com

Why You Need to Know about Your Outsourced Service Provider's Internal Controls

If you're looking to contract with an outsourced service organization, you undoubtedly have many questions about the provided services. Among these questions, you need to be sure to ask about the service provider's internal security and operational controls.

While many businesses assume that all outsourced service providers offer the same level of security, controls in fact vary considerably. You need assurances that your service provider has adequate security controls in place around both business procedures and information technology.

Your service provider's controls also play an important role in your organization's own regulatory compliance efforts. Security controls are essential for compliance with a wide range of regulations covering many vertical industries, such as Sarbanes-Oxley, the Food and Drug Administration's Title 21 Code of Federal Regulations Part 11 (21 CFR 11) guidance, Gramm-Leach-Bliley and the Health Insurance Portability and Accountability Act (HIPAA). All of these regulations require companies to document and manage business and financial processes as well as implement technologies that furnish access control, security and change management. These regulations also require companies to perform annual audits to demonstrate that controls are in place and attest to their effectiveness.

Your organization is responsible for these controls and audits whether you directly control the business operation — or outsource some aspect of its management to a service provider. Thus, in order for your organization to meet regulatory requirements, you need an audit that describes the service provider's controls and whether those controls are up to the task

For these reasons, you need to know about SAS 70 Type II — and about whether the service provider you're considering has achieved this certification.

What is SAS 70 Type II?

The American Institute of Certified Public Accountants (AICPA) adopted the Statement on Accounting Standards No. 70 (SAS 70) in 1992 to demonstrate the existence and effectiveness of internal controls at a service organization. SAS 70 takes the form of an audit — typically performed by a top-tier accounting firm — that reviews and tests the service organization's internal controls over business processes and information technology. The resulting deliverable is a Service Auditor's Report.

Service organizations can choose from two types of reports:

- A Type I report includes the service organization's description of its controls and objectives, and an auditor's opinion on the controls' suitability for meeting the specified objectives.
- A Type II report, in addition to the Type I components, includes a test and evaluation of the effectiveness of the internal controls. The Type II attests to the effectiveness of the controls in meeting the specified objectives over a period of time, typically six months. Initially developed to address the needs of the financial industry, SAS 70 has become an internationally recognized de facto standard for assessing companies that provide outsourced services to all industries.

Why Should You Look for SAS 70 Type II Certification?

While a SAS 70 Type I report tells you that the service organization has established internal controls and what those controls are, only a SAS 70 Type II audit report provides you with:

- Insight into the nature of the service organization's controls and an independent party's assessment of their effectiveness
- Alleviation of the burden and cost of performing your own audit on the service organization

SAS 70 Type II certification is an important indicator of quality. It means that the outsourced service provider's procedures are well-documented, support the delivery of its services and can withstand the scrutiny of an independent auditor not just one time but every day.

What IntraLinks Does for its SAS 70 Type II Certification

IntraLinks is dedicated to providing the highest level of security for our customers. Because IntraLinks built its business serving the financial services industry, our solution meets that industry's rigorous security standards — including SAS 70 Type II. As we expanded into new industries, all of our customers have benefitted from the measures we have put in place.

One of the leading global accounting firms performs IntraLinks' SAS 70 Type II security audits on our controls. These controls have been developed in accordance with best practices from the International Standards Organization (ISO) and Control Objectives for Information and Related Technology (COBIT), which is a framework for information security created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). We have commissioned these audits annually since 1999.

In addition to arranging SAS 70 Type II audits on our own operations, we work only with partners who also commission such audits. SunGard Availability Services plays a key role in the IntraLinks service by hosting our production servers and data. SunGard commissions its own SAS 70 Type II audits, which that document controls that complement and extend our own. These SAS 70 Type II audit reports can be made available to customers upon request.

In performing the annual SAS 70 Type II audit for IntraLinks, auditors perform a battery of security tests on both the IntraLinks application and the hosting environment. These tests take place over an annual period and are designed to validate that the control environments meet their respective security objectives. For example, recent audits have included more than 37 tests on nine aspects of security control for the IntraLinks application. Just a few examples of these tests:

- Sampling to determine that data is consistently and regularly backed up
- Observing unauthorized user access attempts to make sure that access was denied
- Touring server hosting facilities and observing that the use of biometrics and card key access controls as well as surveillance cameras and security guards prevented unauthorized physical access to these facilities

On the basis of these tests, auditors can determine the existence of strong procedures and technologies for meeting our stated security objectives and that all of these controls are exemplary. The following sections describe these controls — which include change management, access control, monitoring, transaction security, virus protection, physical access control, data transmission, application and data backups, and data security.

Change Management

When a service provider releases new versions of its technology and updates system software, it needs to make sure that the update process does not disrupt normal operations or jeopardize data integrity. IntraLinks follows a System Development Life Cycle process that establishes standard processes for authorizing, testing, approving, implementing and documenting changes. Our hosting provider has similar approval processes for changes to any portion of their managed system, including firewall policy changes, hardware and configuration changes, and upgrades to the operating system or databases. These formalized change management processes ensure that potential impacts are thoroughly tested in order to prevent unintended consequences. As a result, IntraLinks can offer the reliability needed to meet service-level agreements and enable clients to address regulatory requirements related to change management.

Monitoring

Continual system monitoring is necessary to identify system vulnerabilities as well as detect unauthorized attempts to gain access to systems. A network-based intrusion detection system continuously monitors and identifies attempted security breaches. Documented procedures help IntraLinks respond to and gather appropriate evidence regarding any security concerns. We also conduct regular threat and vulnerability testing on servers, firewalls, routers and other critical systems using automated scripts and scanning tools to proactively uncover any potential vulnerabilities before they can be exploited.

Online Access Control

Only properly authorized clients and system administrators should be able to access applications and data on a hosted service. IntraLinks has implemented policies, procedures and technologies to properly authorize online access to IntraLinks applications and client data, authenticate users and appropriately limit access rights. Intralinks' application requires active authenticated sessions for all users to grant access, with roles and permissions within the application creating a highly granular authorization scheme. Hardware token-based two-factor authentication is mandatory for all administrative users. Our hosting provider offers a layered approach to security for production servers that includes perimeter security using routers, firewalls and virtual local area networks (VLANs), which enable them to limit access to applications and data to authorized users.

Physical Access Control

IntraLinks' hosting provider has extensive controls that enable only authorized personnel to physically access data centers and other areas that host IntraLinks production servers and sensitive customer data. An automated access control system monitors and controls access to the buildings, data centers and global enterprise management centers. Employee, visitor and contractor access is limited using electronic badge readers, biometric hand scanners and pin keypads. In addition, security guards patrol the buildings that house data centers and maintain a physical presence at each building's main entrance to further control access.

Data Transmission and Virus Protection

Data transmission must be complete, accurate and authorized. IntraLinks requires clients using web browsers to access the IntraLinks service to support SSL 3.0, which uses a Verisign Class 3 digital certificate to authenticate users and 128-bit encryption to ensure that intruders are unable to view information as it traverses the web. Virus protection is fully integrated into the IntraLinks application. McAfee virus scanning software automatically scans files and attachments that users attempt to upload to the IntraLinks application for possible viruses.

Application and Data Back-Ups

Regular backups ensure the integrity and availability of customer data is entrusted to the IntraLinks application. IntraLinks operates from two North American data centers that are built with full system redundancy to eliminate single points of failure and are configured for warm failover. Data is replicated in near real time from the primary to secondary data center. Should the primary site become unavailable for any reason, the 'standby' site becomes primary. A real-time snapshot of IntraLinks client data is copied on a nightly basis. Daily backups are performed by our hosting provider and couriered offsite by Iron Mountain. Production data has a retention period of 35 days for each back-up set.

System availability and performance is continually monitored. Tools commissioned by IntraLinks as well as from our hosting provider are leveraged to proactively monitor the production environment. These tools capture information including, but not limited to, CPU cycle usage, memory utilization, disk space and network equipment performance. Some monitors are enabled to run from multiple geographic locations around the globe and emulate end-user tasks on the application. The hosting provider's real-time monitors allow for proactive component replacement before failure. System alerts are monitored 24/7 both by IntraLinks and our hosting provider.

The data center facilities are protected from natural disasters using fire suppression and power management devices, and the hardware operates optimally through proper monitoring of the facilities' environment. There are also documented procedures for responding to fire alarms as well as failures to power, generators, uninterruptible power supplies (UPS), power distribution units (PDUs) and heating, ventilation and air-conditioning (HVAC) systems.

Conclusion

Not all service providers offer the same controls. You need to make sure that your provider offers an appropriate level of security or your business transactions may be put in jeopardy. IntraLinks' origins in the financial services industry have led it to develop systems that meet that industry's stringent demands for data security. The company continuously evaluates and updates its security policies and procedures, and utilizes a SAS 70 Type II audit to verify that those controls will meet its clients' needs. By subjecting its systems to regular SAS 70 Type II audits — and insisting that our partners do so as well — IntraLinks ensures that our solution provides clients with the highest level of security, reliability and integrity — as well as regulatory compliance.

About IntraLinks

For more than a decade, IntraLinks' enterprise-wide solutions have been facilitating the secure, compliant and auditable exchange of critical information, collaboration and workflow management inside and outside the enterprise. For simplifying business processes such as board of director communications, post-merger integration, acquisition management, corporate finance and legal matter management, the IntraLinks platform can help improve operational efficiency and reduce time and costs while adding increased security and control to your processes. More than 750,000 users across 90,000 organizations around the world rely on IntraLinks including 50 of the 50 top global banks, 10 of the top 10 life sciences companies, 25 of the top 25 law firms, and 14 of the 15 largest private equity firms.

Terms of Use

Although IntraLinks has made every effort to provide accurate information in this document, IntraLinks makes no representations as to, and does not warrant, the accuracy and/or completeness of the information herein or its suitability for any particular purpose. The reader assumes all risk and responsibility for his or her reliance on, or use of, any of the material contained in this document.

ALL INFORMATION IS PRESENTED "AS-IS," AND INTRALINKS DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION, INCLUDING THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. IN NO EVENT SHALL INTRALINKS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST REVENUES OR LOST PROFITS, THAT MAY RESULT FROM THE USE OF THIS DOCUMENT.

1 866 INTRALINKS

New York + 1 212 342 7684
London + 44 (0) 20 7549 5200
Hong Kong + 852 3101 7022

www.intralinks.com