



FEATURE



## How the Rise of SaaS Relates to SOX, SAS 70, and Your Legal Contracts

[By Amanda Finch, Director, Strategic Alliances, Journyx]

The growing popularity of Software-as-a-Service (SaaS) is having a significant impact on data security and regulations compliance. Most companies are concerned — and rightly so — about the legal and security issues raised when company data is located outside their firewall. This article will explain:

- What you must include in your legal contracts to protect your company against Sarbanes-Oxley (SOX) compliance violations
- What SAS 70 Audit Types I and II are, and how they help ensure that companies protect your data
- How to guard yourself against the “1,000 social security numbers on a lost laptop” problem

### SaaS Is Here to Stay

Software-as-a-Service is increasingly popular, and for good reason. Its advantages include a greatly reduced time-to-deployment, low upfront costs (for less approval-process drag), and much less need for scarce IT staff involvement. This results in lower business risk by eliminating “bet-the-company” deployment steamrollers, unpredictable cost spikes, and upgrade or maintenance nightmares. For these and other reasons, major industry analysts predict that 25% of business software will be delivered under the SaaS model by 2011.

The upside to SaaS is tremendous. But the business rewards that SaaS brings are not completely without risk. As companies think about bad things that can happen to their data, they often consider these threats: “phishing,” or social engineering targeting the SaaS vendor; insufficient uptime and/or

scalability of the solution; unplanned maintenance outages; theft of data by SaaS vendor employees; and external system attacks.

SaaS is not necessarily more risky than implementing your own in-house solutions. In fact, it is often much less so when you account for opportunity costs, reduced business agility, and ongoing maintenance. Nevertheless, it is reckless to ignore or overlook a SaaS vendor’s operational and business risk potential. So what can you do to ensure that your company can reap the rewards of SaaS while tightly managing the risks?

First, realistically and systematically assess the risks. What kind of company data will be contained in this particular SaaS system? Then, match the level of risk management to the level of data sensitivity or importance.

### SaaS and SOX

Publicly traded companies have a particular concern about SaaS — namely, its impact on Sarbanes-Oxley (SOX) regulatory requirements. The SOX act holds signing officers responsible for the fairness and completeness of their company’s financial statements. They are also held responsible for the state of the company’s internal controls and must report any deficiencies. An internal control is a process designed to reasonably assure that objectives

can be met in the following categories: financial reporting reliability, operational effectiveness and efficiency, and compliance with applicable laws and regulations.

If SaaS solution data touch the company’s financial statements, the company is responsible for the controls on that software service. This is a daunting prospect for IT executives and staff, whose jobs are on the line where IT controls are concerned. Evaluating and assuring your own controls is one thing — but how can you be sure about your SaaS vendor’s controls?

### SAS 70 Audits

Asking your SaaS vendor for a copy of their SAS 70 audit report is a good place to start alleviating concerns. SAS 70 stands for Statement on Accounting Standards (number) 70, professional guidance issued by the American Institute of Certified Public Accountants (AICPA). The SAS 70 audit report documents and attests to the adequacy and completeness of the SaaS vendor’s internal controls for their service. If your company is subject to SOX requirements, you should require all your SaaS vendors to provide a SAS 70 audit report.

This report is designed to be included in your own audits of controls. Because it is an “auditor-to-auditor” report, it can obviate your own physical audit of the SaaS vendor, saving you time and money.



FEATURE

Even if you are not subject to SOX, you may still find the SAS 70 audit report valuable, since it details exactly what your SaaS vendor is doing to protect your company data. There are two types of audits: the SAS 70 Type I and the SAS 70 Type II. The Type I audit assesses whether the SaaS vendor's internal controls are fairly and completely described, and whether they have been adequately designed to meet their objectives. The Type II audit does the same, but also goes a step further to test the controls in operation.

The Type II is more rigorous and usually preferred; however, many companies begin first with a Type I audit and follow on with a subsequent Type II audit. The additional assurance of a Type II is good to have if you need it; indeed, your own auditors may insist on it. Understand, however, that SAS 70 audits are somewhat new in the SaaS vendor world. Ask yourself: exactly how sensitive is the data in this SaaS system? Do we have the ability to configure the system to control and approve the data it contains? Is the vendor demonstrably on schedule toward the type of audit we need? The answers will help you decide which type of audit report (I or II) you will absolutely need today and later on.

**Mobile Devices and SaaS**

SaaS raises the specter of company data outside your firewall and your direct control. You have processes for your company laptops, PDAs, smartphones, and other mobile devices. But don't forget that working with your SaaS vendor may mean asking them to put your data on their own devices. For example, you may choose to hire vendor staff for initial setup and configuration services. Or, you may place a technical support call to your SaaS vendor, who needs your data to help them reproduce the problem on a test site.

Are you emailing files? If so, should they be encrypted? What devices are used by the vendor? How much of your data would they have on that device? When, and for how long? How are they protecting the device's data? How will it be removed? Will they need access to your system when the problem is solved? The answers to these questions will inform the policies and procedures you'll want to put in place between you and the vendor.

As a customer, you have responsibility, too. Are you configuring your software service to contain sensitive information without assessing whether it is truly needed? For example, are you putting social security numbers into the system only because it has a blank entry field for that item? Putting unneeded sensitive data into a system adds unnecessary risk.

**What You Must Include in Your Contracts**

If your company is subject to Sarbanes-Oxley, your SaaS vendor contracts must require periodic audits of security and data protection controls. Using SAS 70 audit reports is an excellent alternative to auditing the vendor yourself. But simply having the report is no magic bullet. You must read it and understand whether the vendor's controls are adequate in your estimation. Most importantly, your auditors must accept the report.

To protect your data, you may wish to consider the following for any software or managed service contract:

- Uptime percentage guarantees (some companies are putting "clawbacks" into their contracts, specifying discounts for uptime shortfalls)

- Advance system maintenance notifications specifying whom to notify and how far in advance
- Outage notifications that include full problem description and a resolution/escalation plan.
- Documented disaster recovery and business continuity plans
- Data backup procedures, including schedules for incremental and full backups
- Restore procedures for lost data
- Network access protection policies and procedures
- Technical support services and procedures
- Code fix and upgrade procedures
- Procedures for returning or destroying data (some exceptions may be made for secured application backups)
- Regulatory considerations for certain data types (for example, health information)
- Restricting ownership of company data to the company
- Restricting vendor from de-encrypting or viewing company data except when absolutely necessary
- Company data on vendor's mobile devices must be protected in transit and at rest
- Code escrow provisions



FEATURE

- Workforce and physical security procedures to prevent unauthorized access or data theft
- Device and media controls and policies to protect data
- Data transmission security policies and procedures
- System and security monitoring tool usage

The issues raised when software applications are delivered as a service are not new, as many companies must allow data to reside

or travel outside their premises for various reasons. SaaS vendors are now working proactively with their customers to assure data protection, and the customers are reaping the business benefits. Make an assessment of your contracts and policies to make sure you can comfortably welcome SaaS into your organization.

**About the Author**

Amanda Finch is CEO of A.D.V. Group, a company that helps executive and management teams to develop and execute partnership and alliance strategies. Drawing on her expertise in application

development, program management, and business development, she understands the need to minimize "organizational drag" while maximizing effectiveness. As CEO of A.D.V. Group, Finch also acts as director of strategic alliances for Journyx in a contractor role. Finch formulates alliance strategy that is aligned with Journyx corporate strategy and develops alliance programs to execute strategy and drive revenue. Ms. Finch is a Certified Project Manager with eighteen years professional experience and has managed projects for numerous industry and government clients.

EmploymentCrossing is the largest collection of active jobs in the world.

We continuously monitor the hiring needs of more than 250,000 employers, including virtually every corporation and organization in the United States. We do not charge employers to post their jobs and we aggressively contact and investigate thousands of employers each day to learn of new positions. No one works harder than EmploymentCrossing.

Let EmploymentCrossing go to work for you.