

PM WORLD TODAY – PM TIPS & TECHNIQUES – MAY 2008

Managing Your Company's SAS 70 Audit

By Amanda Finch

SAS 70 audits are a relatively new business mandate, but they are coming on strong and fast. If your company provides services to publicly-traded companies (including software-as-a-service), chances are customers and prospects have already begun to ask for your SAS 70 audit report. Companies providing services such as payroll processing, benefits administration, and claims processing, as well as application service providers, are facing the need for a SAS 70 audit.

SAS 70 audits significantly impact your company's operations and market position; hence, they require careful management. This article will briefly describe what SAS 70 audits are, who needs to undergo them, and why. It will make the case for good project management of the audit process. It will also describe the basic phases and activities of the audit process, from beginning to end.

Why You May Need to be Audited

The Sarbanes-Oxley (SOX) Act holds officers of publicly-traded companies responsible for the fairness and completeness of their company's financial statements. The quality of these statements depends on a company's internal controls—processes designed to meet objectives for financial reporting reliability, operational effectiveness and efficiency, and compliance with applicable laws and regulations. The SOX act requires that signing officers evaluate these controls and report any deficiencies.

If your company's services could impact the financial statements of a SOX-affected customer in any way, your company's controls must be covered in that customer's controls audit. This is a daunting prospect; service providers with multiple SOX-affected customers could go out of business responding to audit after audit. The SAS 70 audit is designed to solve that problem. A service provider can choose to undergo only the SAS 70 audit, and then simply send the audit report to any of their customer's auditors who request it.

SAS 70 Audits

SAS 70 stands for Statement on Accounting Standards (number) 70 from the American Institute of Certified Public Accountants (AICPA). A SAS 70 Audit Report documents and attests to the adequacy and completeness of your company's internal controls, relative to the service you provide. It is designed to be included in your customers' controls audit. Because it is an "auditor-to-auditor" report, it

can obviate the need for your customers to include you in their own audits. SAS 70 audits must be conducted by Certified Public Accountants (CPAs) or accounting firms.

It's not hard to know when you need a SAS 70 audit; it will begin to show up as a requirement in sales calls and Requests for Proposals. If your customers and prospects are subject to SOX act requirements, they can't afford the risk of using service providers that are not SAS 70 certified. If you are not yet certified, you will soon see deals and customers slip away—if you haven't already.

SAS 70 audits come one of two ways: as a SAS 70 Type I or a SAS 70 Type II audit. Type I is called a Report on Controls Placed in Operation. It assesses whether a company's internal controls are fairly and completely described and whether they have been adequately designed to meet their objectives; it assesses the controls in place at a certain point in time. Type II does the same, but takes it further—it actually tests the controls in operation over a certain stated time period. Hence, the Type II is called a Report on Controls Placed in Operation and Tests of Operating Effectiveness. As you might imagine, the Type II audit is more thorough and requires more time and effort. The type of audit you need (I or II) will be dictated by your customers and prospects; they know how your services impact their operations, which in turn determines the type of audit they will require of you.

The audit report is accompanied by the auditor's Opinion Letter, which states whether they believe your controls are adequate. An *unqualified* opinion means the auditor expresses no reservations about the adequacy of your controls design or (for Type II audits) their reasonable operational effectiveness. If the auditor finds deficiencies in your controls, you will receive a *qualified* opinion; the auditor will state the deficiencies explicitly in the opinion letter.

Why You Need To Manage Your Audit

Undergoing a SAS 70 audit is a project with many "moving parts." Your company will be called on to provide a great deal of information and documentation. To minimize the drag on your company's key people, you must carefully and proactively manage all aspects of the audit process.

Remember, too, that your company will need subsequent audits (at least annually) to remain SAS 70 certified. Good management of the initial audit project can help subsequent audits go smoothly. Perhaps most importantly, managing the audit like any other business-critical project will give your company the best chance to use the audit for operational improvements. These audits are a deep-dive into your critical processes and policies, painting a very clear picture of operational strengths and weaknesses.

Audit Project Management Approach

First you should deeply understand and clearly communicate exactly what a SAS 70 Type I or II audit is—and why it is necessary—to the key stakeholders and participants. Depending on what your company does, these will likely include the Executive Team and the heads of IT, Engineering/Development, Human Resources, Sales, Strategic Accounts/Alliances, and Professional Services (or your company's equivalent). Don't assume buy-in from the audit participants—work to ensure it, because you will need it. Keep buy-in intact through clear and regular communication and expectation setting.

Then, use tools—namely, your project management software system. Keep a project plan, schedule and budget updated as you learn more about the details of the audit process. Assign resources to the project, and stay on top of their availability. In other words, treat it like any other important project. (Ahem!)

Finally, keep the audit participants focused on the reason for the audit—so that customers will continue to buy your services.

In this article, I'll use some examples from a SAS 70 audit that my company, ADV Group, managed for Journyx, Inc., who deliver their Journyx Timesheet™ software as a service to companies worldwide. Journyx asked ADV Group to manage their SAS 70 audit because they had key Software-as-a-Service (SaaS) alliances and partnerships to maintain. They had also seen a dramatic increase in SAS 70 certification requests from prospects and customers. Although highly simplified for brevity, the examples here are taken from that actual audit project. Simple, generic tools for a Type I audit (a project plan, and a proposal evaluation matrix) can be downloaded from

http://journyx.com/storage/sas70/journyx_sas70_project_management.zip

Phases of a SAS 70 Audit

Simplistically, you can think of it this way: the phases and activities of a Type I and a Type II audit are much the same up to a point; then—for a Type II—the tests of operating effectiveness occur. Since the testing phase activities depend on a company's particular controls, they are hard to generalize here. Therefore, this article will discuss the Type I phases in some detail, and then make some reasonable assumptions about Type II testing.

The phases include: Research and Plan, Issue RFP, Select Auditor, Prepare for On-Site, Participate in On-Site Audit, Review and Approve Audit Report, and Internal Follow-Up.

Research and Plan

Learn as much as you can about SAS 70 audits and audit service providers in a formal research phase, for two reasons. First, you will need to discover how audits are conducted so that you can begin to sketch out the scope and schedule of the audit. Second, you will need to compile a list of candidate audit firms or auditors. For scope, discover exactly which aspects of your service will need to be covered by the audit, and which will not. For schedule, find and contact some audit firms to discuss their approach to the audit process, steps in the process, and general schedule expectations. Include them in your auditor list, unless there is an obvious mismatch.

Ask the auditors: what does my company need to do to prepare? How will you, the auditor, prepare? What information does my company need to provide, and when? Which employees and managers will need to participate? What happens before, during, and after the on-site audit? How long will the on-site portion of the audit take, and who needs to be present? What does a typical audit timeline look like? In what amount of time could we expect a final audit report from the time we award you the audit contract? How are the draft and final reports delivered? What do you charge for a Type I? A Type II? What is the best timing for this and subsequent audits? Do you provide discounts for follow-on work? Lastly, would you like to respond to our RFP for audit services?

Every person who will participate in selecting the audit firm should attend a meeting where all auditor selection criteria are brainstormed, listed, and approved. Selection criteria can include total price, type of billing, and many other considerations. They should also cover how the vendors respond to your proposal timeline and milestones. To illustrate, here is a sample list of criteria:

Auditor's questions on RFP received before due date for questions?

Proposal received before proposal due date?

Cover Letter: Company Name, address, phone, fax? Type of ownership (LLC, PC)? Parent co. if subsidiary? Point of contact info provided? Disclosure of any litigation or mediation?

Cost of Work: Fixed price bid? Not-to-exceed cost on expenses? Price? Price for audit renewals (if provided)?

Background and experience of auditor firm clearly stated?

Audit Methodology: Clearly bidding for SAS 70 Type that you specified (I or II)? Explain exactly how they'll help with compiling the controls list? Is control list assistance included in price? Methodology described clearly and in detail?

Audit Deliverables: At least 3 draft audit reports? 1 bound original of final report? 1 unbound photo-ready final report? 1 electronic copy of final as PDF? Other deliverables clearly listed and described?

Project Plan: Timeline clearly stated? Activities clearly stated?

Project Team: Name of each team member included? Position/level of each member? Years experience on SAS 70 audits noted for each? Years with company noted for each? Number of SAS 70 audits worked on noted? Clear whether team member is subcontractor or employee?

Team Leader identified?

Assumptions, if any, stated clearly?

References: three from last 3 years and from companies with similar business models?

Resumes of all participants included?

Sample contract provided?

Joint proposer or subcontractors clearly identified?

The stakeholders should also decide how to rank and weight the different criteria. Are you looking for the lowest price, period? Do you prefer to use a particular kind of auditor firm, one that may carry more weight with your customers? Are you looking for the most efficient or fastest audit process? Agree now on what is most important for your company.

Translate your new understanding of the audit process into a project plan, schedule, and budget—just an outline with rough estimates will do to start. Keep refining the plan as you learn more.

The internal deliverables for the Research phase are an Audit Firm List (with contact information), an Auditor Evaluation Criteria list, and a project plan, schedule and budget.

Issue an RFP

Use the information you have gathered to write a Request for Proposals (RFP). At a minimum, it should specify the type of audit (Type I or II), a contract term (anticipated time from contract award to delivered audit report), pricing terms, and a project timeline for questions/answers, proposal submission, auditor firm selection, and audit steps. The RFP should outline exactly what your company

would like to see in an audit services vendor proposal. It should closely correspond to your auditor evaluation criteria. In fact, a good auditor evaluation criteria list could serve as a rough outline for your first RFP draft.

Identify the writers and reviewers of the RFP, and plan sufficient time for draft review and modification iterations. Once the RFP is approved, release it to the audit firms on your list. It's best to ask each firm whether they would like to receive the RFP before sending it. Record the date it was sent to each auditor on your audit firm list.

The deliverables for this phase are an approved, final RFP and an update to the Audit Firm List noting RFP send dates for each firm to which it was sent.

Select Auditor

In the auditor selection phase, you will: create a matrix table for evaluating and comparing vendor proposals, answer any auditor questions about your RFP, receive and review proposals, plug information from the proposals into the evaluation matrix, and select an audit firm or auditor.

Good vendor selection processes are considered part of your company's internal controls. Therefore, the selection merits a certain amount of rigor, and should be fully documented. To document your selection process (and also make it easier), create a blank Auditor Proposal Comparison matrix. This matrix is a table with evaluation criteria listed vertically down the leftmost column, and audit firm names horizontally across the topmost row (becoming titles for the successive columns to the right). The leftmost cell of the top row is left blank.

The evaluation criteria in the leftmost column come directly from your Auditor Evaluation Criteria list. The audit firm names across the top row come from your list of auditors; list only the auditors who received your RFP. Building the matrix form in a spreadsheet application makes it easier to move columns and sort the data later on.

If your RFP allowed a time period for auditor questions, you will collect and answer them during this phase. Keep good notes, and use the questions to improve your Auditor Proposal Comparison table if possible. Be sure to also record the date for each question and answer, and the means by which they were received or sent (email, phone).

Note the delivery date for each proposal you receive from an audit firm (was it received by the proposal due date?). Fill out a Proposal Comparison column for each audit firm as their proposal is reviewed. Each cell in the matrix will be filled with relevant data for that criterion—such as a yes/no, a checkmark, a number, or dollar amount. If there are multiple reviewers, they can fill out multiple copies of

the matrix and reconcile them later, or they can collaborate on entering one set of data into a single matrix.

When all proposals have been reviewed and the comparison matrix has been completed, convene the stakeholders for an initial auditor selection discussion. Each participant in the discussion should be provided with the completed comparison matrix. Given your company's particular priorities, the selection may immediately be obvious. If it is not, create a short list of auditors to choose from. Agree on the criteria that inform your selection from the short list. Modify the comparison matrix to include the short list selection criteria. It's also helpful to rotate the short list auditors' columns to the lead, for easy comparison.

In a timely fashion, notify eliminated audit firms of their status. Contact each audit firm on the short list for more information (corresponding to your agreed-upon short list criteria). Give short-listed auditors a reasonable expectation of your decision date, which should (hopefully) correspond to the contract award date specified in your RFP. Convene the selection group again, compare the short listed auditors based on your new information, and choose an audit firm. Quickly notify the eliminated short list auditors of their status.

Inform the winning firm of their selection, and ask for a copy of the audit contract. Identify and notify the people who should review and approve this contract prior to its acceptance. Generally speaking, that will include (at least) one executive level company officer, and the person whose budget is covering the audit fees. Once the contract is signed, ask the auditor to provide you with a letter confirming that they are engaged to perform a SAS 70 (Type I or Type II) audit. You'll be glad you did, because it's almost certain that your sales team will need it to reassure the ever growing number of prospects and customers that will demand SAS 70 certification.

The internal deliverable for the Auditor Selection phase is a completed Auditor Proposal Evaluation matrix; the external deliverable is a signed contract with the selected audit firm.

Prepare for On-Site

To prepare for the on-site portion of the audit, you'll provide the auditor with documentation and descriptions of your policies, procedures, and processes. You'll be asked to document things like your risk management processes, hiring and firing procedures, and security, among others. Many auditors perform an audit-readiness assessment to identify any gaps in information or items that will be needed during the audit. Auditors will also often provide a checklist or sample report to illustrate the information they will need from you.

Some auditors ask you to upload your information to their secure website during the preparation phase. That approach is good for the auditor, and can lower their

costs—the website entries often fill the blanks in an audit report draft—a head start for the auditor. Faster, less expensive audits are good, but you should never simply “type and submit” into these forms, for a couple of reasons. First, any website can have technical problems. It’s frustrating to type in large amounts of information, only to see an error message upon submittal. Second, the information needs to exist separately from the website so that it can be easily reviewed in its entirety at any time. A better approach is to use the website entry form questions to create your own list of information items needed. After you have gathered the information items, you can copy and paste text or upload files into the website as appropriate. Some typical information items are network diagrams, security procedures, development process descriptions, and company policy documents.

Also, review auditor-provided checklists or sample reports, and confer with the auditors to make sure your information item list is complete. Identify all staff members that will need to provide the information items listed. They, and their managers, are stakeholders and participants in the preparation phase.

Assign an expert owner or owners for each information item needed to ensure accuracy. The owners will gather the information items, review and correct, and create any that are needed but missing. Assign someone the task of making sure that every item has been covered.

The readiness assessment, if your auditor provides it, will use your information to determine whether your company has important gaps or inadequacies in the controls or control environment that should be remedied before the audit. If it is uncertain whether your company would receive an unqualified positive opinion, you would be wise to make a readiness assessment part of your preparations.

Designate a file repository (or repositories) for the audit project. In it, file together copies of all information items provided to the auditors before the audit. Label the set of files appropriately to indicate that the information was provided before the on-site portion of the audit.

Confer with information owners, auditors, and all other stakeholders to set a date for delivering the information items to the auditors, and a date for the audit on-site. Ask the auditors which of your company’s employees and other key people will need to be present and available during their visit. Work with the auditors and participants to align all schedules around those dates. Verify and confirm both dates with all parties in writing (email, letter, or other), and keep a copy in the project files.

The internal deliverables for the audit preparation phase are an Information Items Needed list and a project file repository; the external deliverables are the actual information items and a copy of the written confirmation of the information due date and the on-site date.

Participate in On-site

The auditors will visit your company to perform an on-site inspection, speak with staff, and gather information. They will inspect your facilities and your network or data center. They will also ask about your company's division of labor and job responsibilities. These questions assess whether your company's policies and procedures are adequately designed to protect your customers' money and information (not to mention your own).

For a Type I audit, the on-site portion can be a few days. For a Type II, it can be several weeks, depending on the size and complexity of your operations. This is because the Type II audit goes beyond simply listing and assessing the controls in operation. It actually tests the controls over a period of time to determine whether they function properly to meet their objectives. The form of the test corresponds to the type of control activity; for example, if your company has a personnel policy requiring background checks for new hires, the test of this control may be to inspect the background check reports in the personnel files. Or, if your company has a defined customer support process, the auditors might evaluate a sample set of customer issue records to verify their escalation through the process.

During the on-site, you may be asked to provide additional information items. As you provide each item, file the copies in the project file repository. Make sure you label the set of files to indicate that the information was provided during the on-site. If the auditors ask for information after the on-site, file and label similarly to indicate that the information was provided after the on-site.

External deliverables for the on-site audit phase are any information items requested and provided during the on-site. Internal deliverables are copies of those items placed into the project file repository.

Review and Approve Audit Report

After the auditors have performed their on-site inspection and collected all the necessary information about your controls, they will draft your SAS 70 audit report, and provide it to you for review. You should receive both parts: the auditor's opinion letter and the detailed description of controls. For Type I audits, the letter states the auditor's opinion on whether your company's controls are adequately designed to meet the control objectives and the specific date on which the controls were in operation—it is a point in time reference. For Type II audits, the letter will state an opinion on the adequacy of control design, and also contain a statement on whether the controls were operating effectively over a specified period of time.

Before the draft report arrives, identify the reviewers at your company; the list of reviewers should include all the information owners from the previous phase.

Identify the approver of the report—usually the CEO or another executive level officer. Ensure that the review process portion of your project schedule allows at least three iterations of the draft. More would not be unlikely.

Assign reviewers to specific sections of the report by subject-matter expertise—your network administrator won't add value by reviewing the sections on your human resources processes, for example. The subject-matter experts should review for accuracy and completeness of the information. In addition, assign someone the task of reviewing the entire report for formatting, grammar, and typographical errors.

Before the reviews, find out: exactly how does the auditor firm prefer to receive any changes you recommend—by electronic file markup, ink on hardcopy, or other means? Using the process that best suits your auditor's document editors will result in faster and fewer review cycles, even if it seems more cumbersome to the reviewers at your company.

At this point, maintaining participant buy-in will be critical. If your company does not have a rigorous and systematic process for distributed document review and modification, you will feel the pain now. This audit report will be among your company's most important documents; it demands a thorough and efficient process. Design a good process and make sure that all review participants understand and follow it. Clearly communicate the potential problems this process avoids, and the trade-offs you are making. For example, asking multiple reviewers of the same section to collaborate on a single change list avoids change list reconciling. The process should be documented and distributed to the reviewers beforehand (as a memo or email).

Once the report has incorporated all changes correctly, submit it to the approver. Once approved, notify the auditors. They will create and deliver original final copies.

The internal deliverables for the review and approve phase are a list of reviewers, an identified approver, and a review process memo or email. The external deliverables for this phase are the report document change lists provided to the auditors (in whatever form specified), and the approval notification to the auditor for the final draft report.

Internal Follow Up

The audit process does not conclude upon receipt of the final audit report. You must notify the right people within the company that the audit has concluded (hopefully successfully), and that the audit report is available to those who need it. But take care—a SAS 70 audit report contains highly sensitive information about your company's operations and security. Your company should provide it only to

parties with a legitimate need, such as highly-qualified prospects or current customers.

The appropriate parties at your company must create guidelines for distribution of the report, which should include designating a “keeper” of the final report, and a process for requesting and approving distribution. The opinion letter that accompanies the report contains no sensitive details; it can have a wider distribution than the full report. If you need only to demonstrate your company’s SAS 70 certification status, the letter should suffice. If the recipient is undergoing an audit themselves, or if the full report is contractually stipulated as part of a sale, you’ll need to provide the entire report. It may be wise to create a form for requesting distribution of the audit report to an outside party. Disseminate the guidelines to all who may wish to send the report outside the company.

Remember too, that you will undergo subsequent audits to remain SAS 70 certified. Policy or procedure changes must be properly documented, including a full description of the change and its effective date. Changes must be verifiably distributed to all impacted parties. For example, all employees may sign statements confirming receipt and understanding of new personnel or company policies. Or, if your company changes its customer support process, the process diagrams and documents must be updated accordingly, and verifiably distributed to the right parties. Keep document change logs up to date so that future audits go smoothly.

Archive the SAS 70 audit information and documents in one place, and ensure that only authorized personnel have access. Place the SAS 70 final report originals and all copies with the report’s designated “keeper.”

The internal deliverables for the internal follow-up phase are the guidelines for audit report distribution, forms for requesting distribution, copies of these in the project file repository, and the final audit report placed with its designated keeper.

Finally, sit back and celebrate. You’ve survived your first SAS 70 audit!

About the Author:***Amanda Finch****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.