Wednesday, August 15, 2007
Vol. 23, No. 15

Soft•letter

BUSINESS INSIGHTS FOR SOFTWARE DEVELOPERS & PUBLISHERS

A SAS 70 Audit: Should You Make the Investment?

By Pat O'Day, Bluelock

Whether you consider it a competitive advantage or a fundamental requirement, regulatory and security compliance issues are impacting every sector of the software industry. While there are many compliance standards to choose from, they are often dictated by the vertical market your business resides in or supports. If you resell your services or your software, your product will often fall underneath the regulatory requirements or desires of the companies you service. Publicly traded companies have Sarbanes Oxley (generally enforced at the operational level by COBIT), Federal entities have FISMA, Healthcare has HIPAA, Credit Card Processors have PCI and so on.

One standard that seems to be commonly adopted by most service organizations is a SAS 70, also known as Statement on Auditing Standards No. 70. Originally a SAS 70 was designed by AICPA (American Institute of Public Accountants) to provide guidelines in assessing the internal controls of a corporation. These audits were performed by CPAs and focused on the bookkeeping controls looking for accounting errors and anomalies. The process worked well in most regards, so as IT became more critical to the ongoing operations of businesses, SAS 70 began to expand into other areas that fell outside the scope of traditional accounting into more IT specific criteria.

Some of these criteria include backups, physical security access to your servers, whether or not you have a disaster recovery plan, do you follow a secure development or software release methodology.

In evaluating whether or not a SAS 70 audit is right for your business, it's important to understand your objectives. Certainly if you are receiving proposals that require you to have one, the justification is obvious. This is starting to more frequently be the case for two main reasons. The first is the steady and seimic shift of traditional client server software companies into different SaaS (Software as a Service) models shifts software companies into a new service world and puts them squarely into the SAS 70 target zone. Additionally, buyers of software products and especially software services are struggling to find differentiators and are also under increased pressure to improve security, so they add the SAS 70 checkbox to their RFPs.

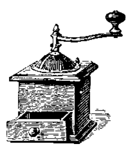
(continued on page three)

Softletter Subscribers, Save $200 on Your Attendance

Softletter's Marketing and Selling SaaS Seminar, 2007

Complete agenda and schedule up on www.softletter.com

Santa Clara, CA October 3/4, 2007



As we grind through the numbers in our Sales Efficiency survey, many interesting trends and datapoints are revealed See pages 2,4-5.

Publisher & Managing Editor
Merrill R. Chapman
rickchapman@softletter.com
860/663-0552

Editor
Donald K. Rosenberg
don@softletter.com
919/687-4172

Editorial office
Soft•letter
34 Sugar Hill Rd.
Killingworth, Conn.
06419
Voice: 860/663-0552

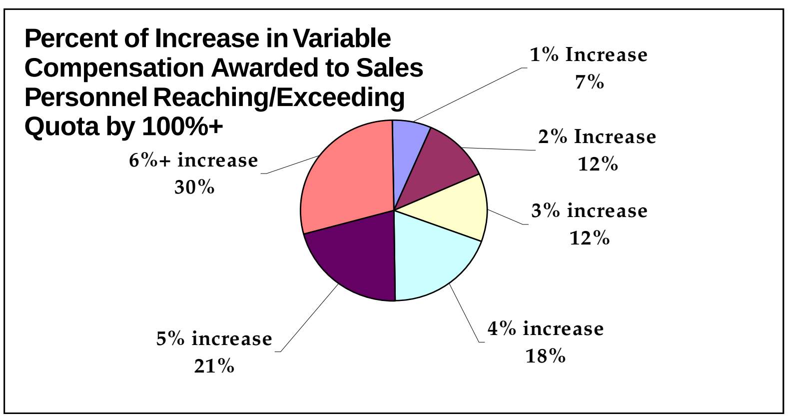
Subscription office
Aegis Resources
34 Sugar Hill Rd.
Killingworth, Conn.
06419
Voice:860/663-0552
Fax: 860/663-0553
info@softletter.com

www.softletter.com

The 2007 Softletter Sales Efficiency Survey: Detailed Analyses

Percentage Over Quota	Increase in Commission (added to standard commission rate)					
	1%	**2%**	**3%**	**4%**	**5%**	**6+%**
1 to 10%	51	23	9	16	24	10
11 to 25%	34	45	31	32	26	24
26 to 50%	25	29	32	17	15	17
51 to 75%	15	9	24	24	16	10
76 to 100%	10	13	14	22	25	21
100%+	10	17	18	27	31	43

Question 16 in our survey was designed to extract a sense for how generously software companies reward their sales people for exemplary performance. The chart below gives a better visual look at how software companies reward their highest performers, individuals who exceed quota by 100%+. Assuming a 5% to 6.5% base, the largest cohort in our study, the addition of 6%+ in additional quota would represent in most cases a doubling in variable compensation. Our analysis shows that 51% of software companies reward sales representatives who reach 100% of quota with at least a doubling of their variable compensation.



Medians of Sales Personnel Achieving Quota By Software Type

Enterprise/Client Server	SaaS	Desktop/Retail	OEM
50%	**58%**	50%	33%

OEM continues to have problems, the Enterprise/Client Server and Desktop/Retail figures are absolutely unremarkable, and SaaS leads the pack by a significant percentage (though the number is by no means dramatic). What accounts for the SaaS lead in this area? One reason may be that the average initial SaaS sale is lower than client server and easier to sell. Another factor is that SaaS sales are typically faster to close, allowing SaaS sales personnel to move on to new prospects more quickly.

(continued on page four)

SAS 70 is broken into two main elements. They are referred to as Type I and Type II. In layman's terms, a SAS 70 Type I is an assessment of controls and control objectives that you currently have in place at a specific point in time. For example, if you have an objective of having secure passwords that would be your control objective. Some controls you may have put in place to help your company achieve that objective might be to have a password policy in your employee handbook, implementing the complex password feature on your servers, forcing a mandatory password change every 90 days, or even offering in-service training on security that would help your employees understand how to manage their passwords. Your SAS 70 auditors will examine these items and document that you actually do have those controls in place to achieve your password security objective.

A Type II report attempts to illustrate that not only do you have those controls in place at a specific time, but that you've been actively using and documenting them over a specific period of time (typically six months). So if you stated in a Type I that you mandated an in-service for every employee once a year on password security, they would want to review a copy of the sign-in sheets or employee records to ensure that was actually the case. The important thing to remember about the controls is that while there are some rough guidelines from AICPA, most of them are at your discretion. One of the features (or flaws) of the SAS 70 is that it is very loosely defined. That means different things depending on your point of view.

"The cost of a first SAS 70 audit can easily reach $100k. But remember that one of the motivations of the auditors will be to drive billable hours. Be prepared to carefully discuss the scope of the audit, what you need to achieve, and what you don't, to control costs."

—Pat O'Day
Bluelockftware

And not all SAS 70's are created equally. Depending on the scope of work defined by the client, a SAS 70 could range from a handful to a virtually unlimited number of controls and control objectives. From the standpoint of your market, providing an option for customers to simply check the SAS 70 box isn't enough. Your SAS 70 report is a document that you should expect and push your clients to read, especially given the potentially significant investment you will have to make to go through and complete the process to obtain that auditor's report.

One very positive note is that this flexibility puts you in the driver's seat in defining the document itself. If you want it to focus on a particular aspect or line of your business, define the scope that way. Ifyou offer multiple software products, some that fall under heavy regulatory scrutiny and others that don't, work with your auditors to fixate the scope only on controls and objectives within that area. This can greatly reduce the cost of your engagement.

If you are concerned about the cost of the process and whether or not it makes sense for your businesses, the best bet is to ask your existing customers. They should be able to tell you if they consider it something important enough for you to spend time on, and better yet, whether or not they would be willing to incur an increased cost for your product as a result. Once the report is complete, not only can you share it with your clients and prospects but they can then use it internally to illustrate what kind of software or service provider they *(continued on page six)*

By contrast, performers exceeding quota from 1 to 10% don't fare nearly as well; nontheless, we were impressed by the generous temperament of the software industry in the aggregate, with 38% of the respondents rewarding our 1 to 10% group with 4% and up increases in variable compensation.

Median Base Salary by Company Development State

Privately Owned	Privately Owned, Privately Funded	Privately Owned, Venture Funded	Public
$62,000	$60,000	$60,000	$95,000

As these numbers reflect, privately owned companies are far less generous with their base dollars; not surprising since they must constantly manage their cash with hawk-like vigilance. Public companies, with piggybanks filled with public revenues and driven by the need to drive stock prices, are far more generous. But when we look at the numbers by company revenue size, we see a more revelatory picture.

Median Base Salary by Company Revenue

Under $1m	$1 to $5m	$5 to $10m	$10 to $99m	$100m+
$60,000	$60,000	$75,000	$75,000	$80,000

As these numbers demonstrate, once a company steps out of the $5 million revenue range, which in most cases represent companies in bootstrap or startup mode, the cost of hiring sales representatives jumps sharply. The reason is simple; if you want to grow, you must pay for the sales talent capable of making that happen. A classic and continuing error companies in the critical $1 to $5 million range make is refusing to recognize reality and attempting to continue to hire sales representatives "on the cheap" as well as failing to adjust their company's mindset to accept the need for sharp-dressed killers who live for the thrill of the close. By the time a company reaches $100 million in revenue its usually thinking IPO and sales compensation rises accordingly.

Average Variable Commission Paid by Company Based on Revenue Size
(Decimals rounded off to nearest number; numbers will not equal 100%)

	Under $1m	$1 to $5m	5 to $10m	$10 to $99m	$100m+
3 to 5%	na	23%	28%	28%	44%
5 to 6.5%	na	25%	20%	22%	22%
6.5 to 7.5%	na	19%	8%	5%	0%
7.5 to 8.5%	na	8%	12%	11%	0%
8.5 to 10%	na	4%	3%	14%	11%
10%+	na	15%	20%	16%	22%

The most interesting aspect of these numbers is the commission "hole" that develops around the 6.5% to 8.5% commission payout range. Apparently, most companies make the decision to follow the traditional 5% to 6.5% spread or opt to offer big payouts, especially as company revenues grow.

(continued on page five)

Medians of Sales Personnel Achieving Quota By Company Revenue

Under $1m	$1 to $5m	$5 to $10m	$10 to $99m	$100m+
78%	50%	50%	50%	**67.5%**

These numbers are illustrative of a couple of points. The high performance of the under $1m cohort can probably be traced to the fact that if you're not doing a good job of sales at this point in your company's life, you probably don't have time to participate in this survey. At the high end, we suspect a company reaches $100m+ in sales because its sales force is able to beat the medians.

Medians of Sales Personnel Achieving Quota By Development Stage

Privately Owned, Privately Funded	Privately Owned, Venture Funded	Public
60%	50%	**30%**

This number was something of a puzzle, explained by the fact that smaller public companies seem to do a bad job of meeting sales goals, thus dragging down medians in this data slice sharply. One reason that might account for this number is that when a small company goes public, it tends to relax a bit, believing it can rely on its fresh influx of cash to carry it; larger companies are too big to be able to indulge in this behavior. This is a number we'll be looking at in closer detail in the future.

Medians of Percentage of Sales Personnel Exceeding Quota By Software Type

Enterprise/Client Server	SaaS	Desktop/Retail	OEM
15%	**5%**	10%	10%

Medians of Percentage of Sales Personnel Exceeding Quota By Company Development Stage

Privately Owned, Privately Funded	Privately Owned, Venture Funded	Public
10%	**20%**	10%

Medians of Sales Personnel Personnel Exceeding Quota By Company Revenue Size

Under $1m	$1 to $5m	$5 to $10m	$10 to $99m	$100m+
0%	10%	12%	**15%**	**13.5%**

The numbers analyzing medians of sales personnel who exceed quota don't reveal any startling numbers, but the comparatively poor performance of SaaS companies when we look at performance by software type is noteworthy. Also note the median performances of larger companies vs. smaller in the company revenue size breakdown.

In the next two issues of ***Softletter***, the **Advisory Board** section will be dedicated to providing further analysis of our survey results.

have entrusted specific elements of their business with. Note that there no restrictions on the publication or use of a SAS 70 report, though, many SAS auditors will imply such restrictions exist. (You may, in the interests of future amity, want to discuss with your auditors any plans you're making to use your audit as a marketing piece.) The caveat in this equation is that only the auditor, you, and your clients are supposed to rely on the report; third parties with whom you have no relationship are supposed to use your audit only for "informational purposes." Thus, developing a white paper tumpeting your SAS 70 compliance for marketing purposes may give your auditing firm heartburn; some SAS 70 firms do attempt to limit the use of their reports in this respect.

"A frequent misunderstanding is that SAS 70 is a certification and that once the process is completed, you're rewarded with a plaque or similar testimony of merit. When your SAS 70 is complete, you receive a report. That's it. The report is the auditor's opinion, nothing more. Their opinion simply states how you compare to a set of controls defined by you and by the SAS 70 framework itself."

—Pat O'Day
Bluelockftware

Another cost control method would be to look for synergy from your suppliers. If you use a particular subcontractor or service provider, perhaps they already have a SAS 70 in place that would cover 30% of your control objectives for a particular aspect of your business. Often companies providing software as a service utilize an outsourced data center facility. The majority of the market leaders in this space have already been through the SAS 70 process in an effort to stay competitive. No need to reinvent this part of the wheel if you don't have to.

A remember that the SAS 70 report is broken up into two sections. The main report is what you typically share with existing customers and potential prospects. Additionally, your auditor should provide a management letter. In this letter, they may list areas that, in their opinion, need further attention. These can include problems that have been uncovered or recommendations that indicate you are not meeting security and privacy controls necessary in your market. You do have the ability to issue a response. So if, for example, the auditors have noted that you don't have security cameras in your facility, but you have planned and budgeted for them to be installed in the next fiscal quarter, you can state this in the response letter, which will be included when the report's distributd. The response lacks the weight of an auditor's "thumbs up," but it does offer you the opportunity to tell your clients and potential customers you are addressing potential issues proactively instead of leaving the assumption you're not taking action out there.

SAS 70 is not a one time process. You should plan on redoing it at least once every two years. A good strategy to control cost might be to audit different lines or aspects of your business once a year and then rotate them every other year. This keeps the process on your mind and in your budget, the scope manageable and doesn't burden you with a another big project and time expenditure every year for you and your staff.

When evaluating auditors who claim that they are able to provide SAS 70 reports, it's important to ensure that they're certified public accountants. Additionally, recognizable "brand names" go a lot further (and cost more) towards making your clients comfortable that you have good controls in place and that your SAS 70 report is accurate.

Pat O'Day, CTO, Bluelock, 6325 Morenci Trail, Indianapolis, Ind. 46268; 888/402-2583. E-mail: poday@bluelock.com

Equities

When is the Right Time to Sell?

By Frank Berger, Corum Group

Some entrepreneurs are forced to sell their company because of cash flow problems, severe illness, threat by competitors, dramatic changes in market conditions, divorce, etc. Some entrepreneurs desperately want to sell their company because of burn-out, the wish to do something totally new in their lives, hassles with business- partners....

But the probability is high that when these companies are sold, it will be at prices well below what the company is really worth because the timing of the sale was determined for reasons other than value optimization. Achieving **optimal** financial results, however, is determined by three parameters:

- Situation of the M&A market in general.
- Situation of the market your company is operating in.
- Situation of your company.

The right time to sell is when all three are at a peak.

We are in the fourth year of consecutive growth in M&A activity, up 30% over last year. Transaction values have been moving up since 2004 and have reached an average high of almost 3.X revenues. Market conditions are still robust and I don't expect the situation to change quickly. If you are considering selling your company, the current climate is very favorable.

If the market your company is operating in is hot, lots of transactions are taking place, consolidation is galloping and maybe a few parties interested in your company have already knocked on your door—that's the right time. Do not accept the first offer on the table. In almost all of these cases, you will be able to achieve a significant improvement over an initial offer. Start the selling process when your company shows good performance—growth above market, good profitability, impressive new wins, etc. Since the normal selling process will take between six and 12 months on average, be sure your company is able to keep up the performance. Deterioration of corporate performance during the selling process almost always has a highly negative impact on a final valuation number.

Frank Berger, regional director, Corum Group, 10500 NE Eighth St., Bellevue, Wash. 98004; 425/455-8281. E-mail: frankb@corumgroup.com.

Company/Description	Acquired by	Price/Terms	Revenues	Multiple
Xansa (XASAF.PK) *• Euorpean IT services*	Groupe Steria (SRIAF.PK)	$962,600,000 *Terms: Cash*	$816.900,000	**1.18**
CheckFree (CKFR) *• Electronic billing/payment & online banking*	Fiserv (FISV)	$4,400,000,000 *Terms: Cash*	$972,600,000	**4.52**
eBaum's World *• Online entertainment*	HandHeld Entertainment (ZVUE)	$17,500,000 *Terms: Cash and stock*	$5,200,000	**3.37**
Infocrossing (IFOX) *• IT outsourcing*	Wipro (WIT)	$600,000,000 *Terms: Cash*	$232,400,000	**2.58**

CardFile

SAS 70 Resources

- **SAS 70.com** (www.sas70.com): The official SAS 70 website. Invaluable repository (except on pricing) of articles on the subject.
- **Polarcove** (www.polarcove.com/whitepapers/sas70FAQ.htm): Site and link offer whitepapers and excellent information on SAS 70.
- **Janco** (www.janco.com): Company provides various print publications dedicated to assisting firms to prepare for various security audits. Prices are not cheap; SOX preparation books, for example, range from $640 to $3200.
- **SAS 70 Solutions** (www.sas70solutions.com/SAS70-Resource-Center.html): Site offers good collection of articles and documents on SAS 70.
- **Compliance Online** (www.complianceonline.com): Site offers both CD- and web-based training courses on preparing for SAS 70 audits.
- **ISO 17799 CENTRAL** (www.17799central.com): Site offers information on ISO 17799, a standard many believe is preferable to SAS 70.

LONG TAIL AUTHOR CHRIS ANDERSON ON THE ECONOMICS OF BUSINESS BLOGGING FOR GUY KAWASAKI: "A best-selling author and genuine tech celebrity writing a thoughtful essay nearly every workday on a top-50 blog for an audience of around 30,000 people/day.

And the pay for that is about $280 a month. If Guy can get Google to write a check at all.

Just another reminder that the reason to be a Long Tail producer is not direct revenues. Instead, it's exactly what Guy uses it for: marketing for his books, VC firm, speeches and consulting. For which he's exceedingly well paid. Indirect revenues rule!" (Quoted on http://www.longtail.com/the_long_tail/2007/01/dont_quit_your_.html, 04/07/2007)

MATCH.COM FOUNDER GARY KREMEN ON THE VISICITUDES OF SILICON VALLEY MILLIONAIRES: "You're nobody here at $10 million." (Quoted in ***The New York Times***, 08/05/2007)

BLOGGER AND DATABASE PROGRAMMER SEAN MCOWN ON MICROSOFT ACCESS: "I've taken a pretty good look at Office 2007 and the new Access, and the one thing that goes through my head is the same thing that goes through every time I see Access... when is MS finally going to just get rid of this thing? What real purpose does it really serve anymore? For tiny shops, you still have to buy it, and MS has other solutions that are just as easy and completely free.

Anyway, join with me and lets all kill Access." Quoted on http://weblog.infoworld.com/dbunderground/archives/2007/08/die_access_die.html?source=rss, 08/08/2007

Colleagues made off with your last issue? Go to www.softletter.com. Click Subscriber Login in the upper right of the home page. To view the current issue and to search archives of hundreds of articles by keyword, topic, or issue date, log in and enjoy!

Soft•letter is published 24 times per year;

ISSN: 0882-3499.

Subscription rates: $395 worldwide. Subscription office: Aegis Resources 34 Sugar Hill Rd. Killingworth, Conn. 06419 Voice:860/663-0552 Fax: 860/663-0553 info@softletter.com

www.softletter.com