


Sarbanes-Oxley

COMPLIANCE JOURNAL

Quick Links

- [Sarbanes-Oxley](#) 
- [US Security & Exchange Commission](#)
- [New York Stock Exchange](#)
- [NASDAQ](#)
- [American Stock Exchange](#)
- [COSO - The Committee of Sponsoring Organizations of the Treadway Commission](#)
- [Public Accounting Oversight Board](#)



[Advertise with Sarbanes-Oxley Compliance Journal](#)

Features

[< Back](#)

Sarbanes-Oxley : Technology / Internal Controls

SOX Compliance Dos and Don'ts for CIOs

February 26, 2008 12:00 PM

It is important to remember that any compliance effort requires the cooperation of people, and people are imperfect.

By: [Andrew Gelina](#)

The issues of controlling processes, securing financial data, auditing, and managing document lifecycle, retention, and destruction have become top priorities for CIOs striving for Sarbanes-Oxley compliance. With most offices heavily relying on electronic documents and data, it is essential for companies to have a strategy for managing compliance as it relates to Section 404 of the Act. Here are some simple, but often overlooked do's and don'ts for CIO's who are faced with the challenge:

DO

Start with good governance within the IT department

Start with the IT department and look at what controls exist and which ones should exist. Implement governance in your own back yard first, pretending you are a separate "company within the company.". Note the challenges you face, like system and process adoption, peoples' resistance to change, and technical hurdles. Dealing with these issues diplomatically and with deliberate strategy will help when you have to manage by influence in other areas of the company that don't report to you.

Tackle financials next

Begin your next step working with providing auditing and controls on financial systems. Get the CFO and his reports on board, and let them know a SOX-compliant protocol for processes and procedures is coming in advance and won't disrupt their ability to conduct business, but rather help to improve systems. Progress outward to the (often ad-hoc) systems that feed the financial systems, such as spreadsheets and reports and leverage tools like Microsoft SharePoint Server, which can automate the controls over access to these documents, version control, workflow, document lifecycle, and archiving.

Build consensus

To ensure system adoption and use, work across departments to collaboratively define the



goals and rules of the compliance process, as well as the processes and procedures to be followed. If people don't have a say in the creation of the rules, they are less likely to follow them. Taking a "top-down, bottom-up" approach will help get people on board. If you skip either the management or rank-and-file people in a department, you risk being subverted. All should be made aware of the ramifications for not adhering to the new protocols.

Fight fire with fire

Leverage technology to help solve the compliance issue. Technology created the problem of managing electronic documents, and many good tools exist (some you may already own) to help manage compliance. SharePoint is one such tool well-suited to the tasks of document management mentioned above, and to many other collaborative business tasks. By specifying security settings, storage policies, auditing policies, and expiration actions for business records in accordance with compliance regulations, you can help ensure your sensitive business information can be controlled and managed effectively. Leveraging the right technologies can reduce litigation risk for your organization. Tight integration of Office SharePoint Server 2007 with common desktop applications means that policy settings are rendered onto client applications in the Microsoft Office system, making it simpler for employees to be aware of and comply with regulatory requirements.

Surface the data

Make sure your solution provides dashboards for accounting and operational data. It should be easy to monitor ratios, keep an eye on actual versus forecast data, and flag any out-of-control metrics early. If people don't feel like they can have a handle on the process on a day-to-day basis, and see and feel how things are changing, they probably don't have control. A well-developed dashboard that allows someone to easily see in red and green arrows how various metrics are holding up at the company makes things easier to manage. It also helps people visualize large, complex amounts of data in an easy way. Our brains like to make complex things simple in order to deal with them, and this process helps immensely.

Show me the proof

Make sure your solution is auditable. If you can't report on it, prove it, and guarantee your data integrity – in real time or historically - your compliance effort effectively did not happen. Periodically pretend you are an auditor and look at your compliance initiative. Try to poke holes in it. If you don't feel objective enough to do this, do a trial audit with a consultant before you conduct a real audit. Have department heads do the same after ensuring the Finance department has shared the aspects of their business that are subject to most compliance scrutiny.

Keep it simple

Define workflows that help enforce rules, but stick to what you need. Avoid over-engineering. When using extensible tools, there is a temptation to extend them quite a bit. Couple this with some relatively complex workflow and you can end up engineering a Cadillac when you need an Aveo (and some slight changes to your process). You may decide that automating 90% of the process, as well as changing the process just a bit, is easier than building 100% of the current process.

Re-use

Leverage your existing authentication systems (Active Directory, LDAP, etc.) for your compliance system. You are going to need to prove that only authenticated people accessed the system, so don't write another separate authentication system (and force people to manage another password). It has become MUCH easier to integrate Active Directory into applications to achieve Single Sign On, so don't re-invent the wheel. This applies to both web-based and

Sarbanes Oxley Audit

Use our free checklist to evaluate c
internal controls.

www.softrax.com/SOX-Audit

Sarbanes Oxley template

Free Risk Rating template in Excel
based approach to SOX

www.SarBoxPro.com

Sarbanes-Oxley Readiness

Ex Big-4 CPAs: Process Docs Writt
Gaps Identified, Remediated

www.TheFastTrackGroup.com

Windows client systems.

Find someone who's done it before

Engage experts to help with your project; that is people with experience in Sarbanes Oxley compliance, and people with experience in the technologies you will use to comply. Leverage their experience and perspective derived from working with several different compliance implementations. It's hard to get it all right on your own the first time out. Outside perspective, coupled with the lessons learned (from both successes and mistakes in prior implementations), make consultants valuable in this process.

Get organized

SOX is not a one time problem like Y2K. So it makes sense to organize your reporting, controls and monitoring into a regular business as usual activity. Using a compliance calendar, schedule your monitoring and reporting activities. That way when the year rolls around you have the evidence you need to report to the board.

DON'T

Drop a bomb

Do not try to roll a big, comprehensive solution out to everyone at once. Plan to iterate; pick a small group of users and prototype the tools and processes. Learn from your first implementation, improve, and roll out to a wider audience. Repeat this process, learning from the previous implementation. Each successive department rollout will go more smoothly, and you carry less risk per implementation. Rolling out to everyone at once may at first look less expensive, but will often take longer and cost more to get everyone up and running.

Automate before analyzing

Do not automate every current manual process without rethinking it first. Virtually any paper process can be replicated in digital form, but consider ways to streamline and install automated controls in the process as part of the exercise. Delivering a compliance implementation is a good thing that allows the company to avoid problems, but if you can save money at the same time everyone is happier and the savings go right to the bottom line. Finding enough opportunities for optimization helps offset the cost of the compliance implementation!

Forget about document images

Don't forget about faxes, signed copies of documents, and digital signatures, which are all first-rate factors too. You'll at least have to capture/manage signature pages, which may be managed through a scan-to-PDF or fax-to-email gateway. You may have every revision of the Word doc for drafting a contract, but the executed version is what counts. Store them in the same repository. Consider embedding watermarking or version IDs in the headers/footers of documents to tie signed images back to electronic draft originals. Seeing that the last checked-in version of the contract was 1.15, and the signed version has "Version 1.15" in its header, will help speed up your audits.

Shoehorn

Don't force the fit. Find the right tool for the job - one that manages document versioning, retention, legal holds, and compliance with auditing/reporting. Don't try to adapt a tool or set of tools that are not meant for it. Many times, CIOs will spend tens of thousands in human labor to try to get something done with cheap tools, instead of spending a little on the right tools. You don't see contractors building houses with tools from the Dollar Store. Professionals realize that good tools save them time, are safer, and achieve the same outcome for compliance efforts.

Rely on disaster recovery

Don't rely on your disaster recovery data backup strategy (tape, etc) for compliance. While you may run backups and need to follow procedures during backups as part of your compliance strategy, you cannot say that implementing disaster recovery covers your compliance needs too. Don't count on DR for archival purposes, or for "freezing" or "snapshotting" data for compliance efforts. Use a separate store for these. On the flip side, if you have a disaster and have to cut over to your backup site, you need to follow your compliance procedures there as well. You don't get to skip compliance because you are in DR mode.

Rush to completion

Don't sacrifice diligence and governance in the name of "getting it done." This applies to both implementing your initial compliance process as well as maintaining compliance while managing other projects at your company. If you set extremely aggressive deadlines for each piece of your implementation, you are likely to cut corners and have re-work. It's better to figure out inefficiencies and areas of risk early and bite the budget bullet to ensure you have enough resources to complete the project in a realistic timeframe. Once your compliance program is implemented, you will find out how well you institutionalized its use. People will be pressed by deadlines on their projects and you will quickly see whether the processes put in place are still followed when time is short. If things are well-designed, the overhead will be minimal. If people start to blame missed deadlines on the compliance overhead of their process, you will have to work with them to help minimize the time it takes and/or get this time factored into their project estimates.

CONCLUSION

The Dos and Don'ts outlined above do not comprise an exhaustive catalog of everything you need to remember or avoid during a compliance effort, but they provide some good guidelines for those facing the challenge. Many people (especially from a technical or financial background) will tend to focus on tool selection, technical implementation, and shooting for a mythical "perfect, problem-free implementation" the first time. It is important to remember that any compliance effort requires the cooperation of people, and people are imperfect, and require coaxing and coaching. The better you account for handling the soft areas of compliance adoption, as well as the hard technical details, the smoother your implementation will be.



Andrew Gelina
CEO
Syrinx Consulting

Andrew Gelina brings more than 12 years of software architecture and development experience to his role as CEO of Syrinx Consulting, where he is responsible for the strategic direction, technology focus, operations management, and growth of the firm.

Syrinx is a software development and consulting firm that brings a deep understanding of Microsoft technologies including .NET and SharePoint 2007 to organizations that

are dependent on technology for competitive advantage.



[About Us](#)

[Subscribe](#)

[Editorial](#)

© 2008 Simplex Knowledge Company. All Rights Reserved. | [TERMS OF USE](#) | [PRIVACY POLICY](#)