



Compliance – Year 2 and beyond

*Doing it more easily, more effectively, with **less pain and lower cost***

When building something for the first time experience tells us to 'be prepared to throw the first one away'! Those of us involved in Sarbanes-Oxley compliance can certainly relate to this – who would want to do Year 2 the way we did Year 1? Our researchers interviewed executives from 470 different companies, including 437 compliance managers, 22 software providers, 3 research firms, 43 auditors, 32 CFOs and 19 CEOs.

We have analysed and cross-referenced their responses into this executive summary – things to consider when selecting compliance software or comparing vendors.

In the beginning it seemed difficult to grasp the meaning of what 'SOX compliance' actually meant. Being focused, specific and delivery-orientated one quite reasonably assumed that there would be a definition; some way of understanding how you would actually know that you had 'finished' becoming compliant. At the very beginning auditors were repeatedly asked "what exactly does 'being compliant' mean?" The answer? It turned out that 'being compliant' actually meant 'giving the auditors comfort' – not exactly something that thrilled compliance managers around the world.

Managing the detail is important, and can be difficult. Your boss always wants to know the answer to the question, "How done am I?", and expects the answer to be something like, "We're 62% done boss, and 90% confident of finishing on or ahead of schedule. No obvious road blocks in sight". Most of the people we interviewed told us that, for them, such a scenario would have been inconceivable. Usually, in the heat and sweat of the compliance effort, the only real way they had to know 'how done' they were was by the assessment of the auditors, and often only in terms of how many issues and remediation initiatives that were outstanding. And get this – on the whole, only the auditors actually knew!

Somehow most of us made it through the first year...and into year two. Do you remember the meetings? The spreadsheets? The status reports? The issues lists? The remediation meetings? The awareness sessions? The perpetual conversations with the external auditors about what, exactly, constituted 'evidence', and the arguments with the internal auditors over what the external auditors do and do not actually care about? And the promises to yourself of finding an easier way to make this all work?

If so, you have probably been looking into automating the corporate compliance process as much as possible. Perhaps you have come across the compliance tools that are 'recommended' by the auditors (funnily enough, usually their own and, cleverly, implying that it will be much easier for them to 'gain comfort' from such a system). The problem with almost all compliance-related systems that are available today is:

- a) they are auditor-specific,
- b) they are procedure, legislation or standard specific,
- c) they focus on automating only a part of the process of becoming compliant
- d) they do not take into account associated, or 'spin-off' work,
- e) they are data-based rather than user-based,
- f) they isolate compliance work from 'business as usual' work – often there is no difference.

In many cases the compliance programme manager will have an audit or accounting background, but not always. Inevitably each individual will bring their normal *modus operandi* to bear on the new compliance situation and, consequently, their operating models... In many cases, the compliance initiative falls under the remit of the finance department, but again, not always... Sometimes compliance is part of a wider corporate initiative, sometimes it is stand-alone... Given this mix and the realisation that, for most companies, 'becoming compliant' means different things to different people, how do you begin to address simplifying the activity of becoming 'compliant'?

Our researchers interviewed 437 compliance managers, 22 software providers, 3 other research firms, 43 auditors, 32 CFOs and 19 CEOs, from a combined total of 470 different companies. We analysed and cross-referenced their responses, synthesised their recommendations and collated their insights. The findings revealed several key points to consider when selecting compliance software or comparing vendors:

Think holistically

The process of becoming compliant covers a broad spectrum of activity – understanding processes, designing policies, positioning, executing and monitoring controls, gathering evidence, identifying risks, raising issues, initiating requests for remediation work, monitoring the progress of remediation work, understanding dependencies and mitigating circumstances or controls, and – of course – understanding 'how done' you are. Any software package you choose to help with compliance should, if possible, enable all of these aspects in the same environment.

Automate workflow and process

The processes involved in notifying control owners when it is time to execute a control, deliver evidence or take some step in the compliance protocol is best done automatically, rather than rely on people chasing. That way the compliance manager/officer can monitor the progress of compliance activity in real-time rather than having to continually send emails and reminders (and listen to excuses of 'why it can't be done'). If the workflow in your system of choice, in the case of non-execution, also escalates to the controls owner's boss, then so much the better. This will remove personalities from the equation and give the compliance manager/office more kudos and authority. The same principle holds true of the depositing of evidence, reports and status information – the more automated any of the necessary processes are then the easier, quicker and ultimately cheaper compliance becomes.

Transparent information

Keeping everyone informed and in-the-loop is important. In compliance, as in all other walks of life, if people do not know what you are doing and the compliance status of your organisation, then they will make up their own conclusions. If you have gone the distance to choose a great system which will automate much of your work, then take care to ensure that it is a 'role-based' system so that you can assign users whose sole interest is to see what is going on. This single attribute will save many meetings, status reports, misunderstandings and sleepless nights.

Understand 'doneness'

In the realms of compliance information nothing is as important as knowing 'how done' you are. A truly useful system will push this information at you the moment you enter the compliance part of the system. Graphical displays are best because they are easier to absorb quickly and can convey rich information at a glance. Context is important too, so make sure that you can drill down and see 'how done' all the parts are. If your company is a multi-national you might want to make sure that you can drill in and out of countries and regions and that your chosen system can cope with the complexity of your global organisation. Getting this right is a huge win - you should be able to see the compliance status of your organisation as a whole and drill down to the smallest entity, all from the same place and using the same rich levels of information



Keep the auditors informed (Give auditors a pre-view)

Not everyone agrees, but most think it is easier to keep the auditors involved at all times and to be as transparent as possible. The earlier the auditors can see what you are doing the easier it is for them to plan their activities and to keep their work short and sweet (i.e. cheaper for you). If you can find a system that gives user access to the auditors on their request then so much the better. Not only will they get a good feel for the progress and integrity of your own efforts, they will also accumulate a degree of confidence in your level of control that will result in lower audit fees for you.

Continuous compliance

Talking about compliance as if it is a 'snapshot' event is now obsolete. Continuous compliance is what is required, even if the audit event is a 'snapshot'. Continuously exercising, monitoring and measuring compliance levels is needed and, usually, demanded. Be sure that the system you use is as 'real-time' as possible, that it is well structured, that it accurately reflects your organisational structure and controls, and that is deployed and used dynamically and 'continuously'.

Conclusion

Think 'big-picture' and consider how and why controls are important to you; Grab any chance you can to kill several birds with one stone and find processes that can be automated as you find solutions to compliance problems – the pay back is worth it; Ignore your natural instinct to hide unpleasant news, especially from the auditors, as the details will always surface eventually; Figure out your own completeness metrics and organise your projects in such a way that you always know how 'done' you are; Remember, compliance to regulations, standards, policies etc. will not go away – choose a vendor that knows how to look after you and then sit back, enjoy the ride and see if you can slash auditor fees by making their life easy!



About the Author

Mike Henry is the CIO of Elix-IRR and leads the Programme Advisory division of the business.