Sarbanes–Oxley: 15 Years Later

A Reflection and Examination of Sarbanes–Oxley Requirements and Best Practices

INSIDE THIS PUBLICATION:
> Leverage the SOX risk assessment for improved enterprise risk management
> Increase efficiency and effectiveness of internal control testing
> Eight items you still need to know about SOX
About MIS Training Institute:

MIS Training Institute (MISTI) is the international leader in internal audit, IT audit, and information security training and conferences with offices in Boston, New York, and London. MISTI’s expertise draws on experience gained in training more than 200,000 delegates across five continents. Helping internal audit and information security professionals stay at the top of their game has always been at the core of MISTI’s mission. To that end, MISTI has developed and focused its vast variety of training courses, events, newsletters, and other informational products on the wide-ranging needs of internal and IT auditors and information security practitioners. MISTI’s unparalleled course curriculum covers the most up-to-the-minute topics, provides proven internal audit and security practices, and delivers the information needed to be successful in today’s organizations. www.misti.com

About SOXHUB:

SOXHUB is a SaaS technology company revolutionizing enterprise SOX, operational audits, and audit management software. With SOXHUB, enterprises can collaborate, manage, analyze and report on critical internal controls data in real time. We offer a full suite of audit management solutions for SOX management, ERM, operational audits, and workflow management. SOXHUB’s clients include industry-leading pre-IPO to Fortune 50 companies looking to streamline their accounting and audit functions.
INTRODUCTION

The Sarbanes-Oxley Act seemed like a good idea when Congress enacted it 15 years ago. In fact, when one looks at the data since then, SOX has been a good idea. It did exactly what Congress wanted SOX to do: make financial statements more reliable.

That said, the execution of this good idea has often been terrible. Hence, even after 15 years of implementing SOX and pondering effective internal control over financial reporting, companies still have much they can do to make the experience more useful.

This e-Book looks at SOX compliance past, present, and future. The first article picks out eight points about SOX that compliance professionals might want to remember. For example, the totality of the law was about much more than assessing and auditing ICFR; it was about establishing greater corporate accountability for reliable financial statements. Stronger ICFR is one mechanism to achieve that, but so are whistleblower hotlines, clearer responsibilities for the audit committee, and much more.

Second, our sponsor SOXHub explored the principal challenge for SOX compliance officers today: testing key controls. How can you reduce the number of key controls, to reduce the amount of testing and documentation necessary? How do you train your audit team with the proper skills, and leverage technology to streamline the actual labor of testing and documentation as much as possible? The compliance community has made great strides on that front since SOX debuted in 2002, but modern organizational complexity means the challenge never goes away.

And third, given all the hard-fought experience SOX compliance officers now have—can’t we take that expertise and use it for other purposes that benefit the enterprise? Our third article examines important practices in risk assessment for SOX compliance, to see how they can be applied to other enterprise risk management efforts. In the past, boards often asked whether SOX compliance meant the company was “doing ERM.” No, it doesn’t. But SOX compliance practices do lay the foundation for ERM efforts that come next.

We hope you find this e-Book useful. The central premise of SOX—stronger control over financial processes to reduce the risk of fraud or error—is here to stay. The principles and practices cited in this e-Book are likely to be as useful in the second 15 years of SOX compliance as they were in the first.
When Sarbanes-Oxley compliance arrived in the 2000s, many companies were forced for the first time to assess financial reporting risks and develop stronger internal controls to manage them. Little surprise, then, that as companies went through the experience, some senior executives would ask whether that meant the company was “doing ERM.”

The short answer is no; SOX compliance only addresses financial reporting risks. Enterprise risk management is another level of complexity.

The more thoughtful answer, however, is closer to “not really”—but effective SOX compliance does give companies a leg up to get there.

Now, 15 years into the SOX compliance era, ever more boards, CEOs, and risk managers want to leverage all that investment and spring into ERM. The time and money spent on analysis of business processes, streamlining controls, assessing risk, managing audits—what foundation does it lay to help corporations keep a stronger grip on other risks and compliance obligations, beyond SOX?

A solid one, in several ways.

First, remember that the Sarbanes-Oxley Act compelled the audit committee to take more responsibility for risk management. Sure, in the first few years of SOX compliance, those audit committees dwelled on the details of financial reporting risk and what should be in scope for a SOX audit. Arlene Nelson, a principal at Primary Process Controls in Houston, describes the “basic fire drill” of SOX compliance in the 2000s as “let’s get what we can, identify it, put some controls in there, and get the message out.”

For many companies, those growing pains have passed. New issues have crowded onto the audit committee’s plate—and the art of managing those issues bears strong resemblance to earlier SOX challenges around internal control over financial reporting. The risk assessment techniques honed under SOX can apply here, to improve an organization’s management of enterprise risks.

**MAP IT OUT**

The key step for any SOX risk assessment is to understand the business process in question: to map it out, using flowcharts or narratives that break down a process into its component parts, and identify all the risks along the way. Risks for what? In a SOX risk assessment, risk for material misstatement of financial results. For enterprise risk management, the risks can be much more diverse. But the steps are the same, and even the tools can be the same.

Take the rise of cloud-based data storage providers as one example. Most business executives in the operating units do grasp that service providers can pose serious risks. They use service providers anyway. The question is how they find and use the providers, and what that means for risk.

If the answer is some version of “employee finds vendor via Google search, begins storing company data in cloud after $9.95 charge”—that speaks volumes about the risks the company has (data security and data privacy, to name only two), and the types of controls that the organization will need to add.

Or consider anti-bribery risks from the Foreign Corrupt Practices Act. Most of the enforcement risk comes from third parties acting on a company’s behalf in overseas markets. Therefore a risk assurance team examining FCPA risks will want to understand the company’s process to find third parties and bring them into its extended enterprise.

Finding the process owner, understanding the process, flagging risks to each step of the process: those are time-honored ways of unpacking a risk into its component parts.
CONSIDER THE CONTROLS, ENTITY OR OTHERWISE

After a risk is mapped out, a next logical step is to identify entity-level controls that address it, and lower-level controls at the transactional level to reduce the risk if the entity-level controls don’t work.

Let’s return to anti-bribery risks. Entity-level controls might include clear policies against using resellers or agents in emerging markets where any of the principals are “politically exposed persons.” It could require the use of an outside service that performs background checks on third-parties overseas. The company might even structure its operations to avoid using agents entirely in high-risk countries.

A sophisticated risk assessment, however, must consider what other controls can backstop that risk, should the entity-level exhortations against bribery fail. At the transactional level, such a control might be policy that all payments to third parties in emerging markets must be approved by a business unit president; or all payments to third parties in high-risk countries are held until the party certifies anti-bribery training.

Another example could come from supply chain management. Say the objective is “avoid sourcing any components made by slave labor or human trafficking.” Entity-level controls could include training procurement managers on how slave labor typically works in emerging markets, so they know what red flags to monitor; plus a suppliers Code of Conduct that requires them to certify their goods as slave-labor free. Transaction-level controls could include regular audits of critical suppliers, to ensure that none might cause business interruption if they turn out to use slave labor and are dropped from the supply chain suddenly.

Regardless of the specific enterprise risk, the steps to assess it are the same that exist for SOX: assess entity-level controls; see if their design fits the risk in question; consider what other controls at the transactional level can achieve the same objective, if the entity-level control is insufficient.
TIE IN THE EVIDENCE

After assessing risks and identifying the entity-levels and transactional controls to address them, the other critical task for SOX compliance is to audit their effectiveness. That means determining what tests or audits to perform, when to perform them, and what evidence to collect and document.

For audit and internal control executives, this is a process challenge: how do I audit all this, to gain the assurance the organization needs about the risk? Which locations require independent testing, and which can make do with self-assessments and reporting? How do I take the results and report them to the proper business executives in the proper ways? The evidence required for each of those questions arises from the risks defined in earlier phases. For example, which locations require independent testing? The ones with the most reliance on foreign agents to resell the company’s products. Where can we rely on self-assessments? In places with senior executives who receive extensive training, who oversee processes with low regulatory enforcement concerns.

Those questions hold true of any risk management effort, well beyond SOX and financial reporting risks. Technology helps immensely; documenting evidence in a spreadsheet is just as tedious and error-prone for sustainability, anti-bribery, or supply chain availability, as it is for financial reporting.

SIMPLIFY

Most companies learned Sarbanes-Oxley compliance the hard way in the 2000s, through exhaustive, manual testing and documentation of financial controls. Then came the push to simplify internal controls down to fewer, more key controls; and simpler, more automated processes, both to reduce compliance burdens placed upon process owners and to accelerate the testing and documentation work done by auditors.

One prosaic example: certifications from business process owners that, yes, they have tested the controls assigned to them and that all controls work effectively. Once upon a time, SOX compliance teams chased those certifications via email, collecting and documenting the replies in a spreadsheet. Some companies may still do that.

A more modern approach is to use web-based certifications, where each process owner has a unique URL he or she visits to submit a certification. That accelerates the process of gathering self-assessments: no more manual chasing process-owners missing certifications, no more double-checking that they didn’t alter the form of the assessment. In turn, the risk assurance team now has more time to analyze data from those self-assessments (How many admit deficient controls? How many don’t include appropriate evidence?) or even to analyze risks that emerge from the self-assessment process itself (Why does the Texas office always submit assessments exactly two weeks late?).

REMEMBER THE HUMANS

Those innovations in simplification, automation, reporting—they work irrespective of the risk in question. They are advances in tools and process. They can apply to all sorts of risk that an enterprise wants assess and manage. Plenty of vendors offer technology and advice to help organizations tackle that end of risk management effectively.

The most difficult part of managing risks, financial or otherwise, is people. The biggest challenge for risk assurance executives is simply to have the right conversations with the right people, from the audit committee to the 1st Line of Defense business executives, to process owners further down the chain of command.

Audit committee members might understand industry risks, but not transactional risks. Process owners in one function (say, sales) might know how to circumvent internal controls in another (procurement, trying to block unauthorized vendors). People know when an objective doesn’t make sense, when entity-level policy doesn’t address their daily business concerns, and when transactional-level controls don’t work as designed.

Those truths became painfully apparent in the early years of SOX compliance. The best practices to manage them have improved immensely since SOX arrived in 15 years, and those practices can be applied to the wide range of enterprise risks that weigh on boards’ and CEOs’ minds today.

Which is good news, because the complex, interconnected risk environment for organizations today will only get even more complex from here.
Testing Key Controls

By Peter Yi

INTRODUCTION

This year, the Sarbanes-Oxley Act turned fifteen. Since the landmark law passed in 2002, audit testing procedures have reached new heights with the evolution of testing methodologies, incorporating data analytics, developing new interpretations of “best practices,” and continued changes within the regulatory landscape. While this audit evolution has brought a positive impact to the financial integrity of companies, this has also come at a great cost to the organization and its people.

As shown in Protiviti’s “2016 SOX Compliance Survey:
- SOX audit hours continue to go up
- Co-sourcing relationships are on the rise
- Control counts continue to increase
- External auditors continue to ask for more documentation

To this day, organizations and audit teams are continuously reminded to meet aggressive budgets, identify testing efficiencies across every facet of an audit, and maintain high quality. Meeting such high expectations is difficult for even the most veteran auditor, let alone the new generation of auditors who have joined the profession post-SOX.

How can audit teams strive to improve the efficiency of their SOX programs while staying within budget and accommodating the latest industry regulations and standards? More importantly, how can audit teams free up time and resources in their SOX programs so that they can focus on adding more value to their organizations?

Auditors who can implement any one of the following strategies: the reducing the number of key controls, spend time training team members on both technical and soft skills, and those who leverage technology to improve the audit workflow, should yield both improved control coverage and lower costs.

STRATEGY 1 - REDUCE THE COUNT OF KEY CONTROLS

Organizations face countless risks on a daily basis. Audit teams often address these risks by applying a brute-force approach and simply creating a new control whenever a new risk is identified. Inadvertently, each new control is often classified as “key” without performing a true risk assessment, which then contributes to the ever-increasing count of controls. By understanding the differences between key and non-key controls, internal audit teams can effectively combat rising control counts and “scope creep”.

A control is deemed a non-key control if the potential impact to the financial statements upon its failure is deemed immaterial and if that failure cannot cause the entire process to fail. Conversely, a control is deemed key if it addresses a risk of material misstatement, a high risk, or both a control objective and an assertion. These controls must operate effectively to provide reasonable assurance that the risk of material errors will be prevented or timely detected.

To keep things simple, the quickest method to differentiate a non-key vs. key control is to refer to the level of risk being addressed. Is the control mitigating a low or high risk?

It’s not uncommon to find inexperienced auditors testing controls that address low risk assertions without conducting a mature risk assessment of their environment. Simply assessing the risk level of a control at the account level may lead auditors to add unnecessary steps into their audit cycle, eating away at their limited budgets and timelines.
understand the process flow end-to-end. Often the auditor is ill-informed or limited on time and will test controls in the same manner as prior years to simply avoid drawing attention to themselves. Such oversight could have been resolved if the team developed and analyzed a quality flowchart and discussed the matter internally amongst themselves.

As prescribed by the PCAOB’s Audit Standard 5 (AS5), a risk-based audit approach dictates that companies and their auditors focus on areas of high-risk. As a best practice, audit teams should make an effort to plan and perform a recurring risk assessment and controls rationalization exercise annually. Doing so can help train team members to better understand their organization while identifying opportunities to reduce the scope and focus attention on areas that matter most.

**STRATEGY 2 - TRAIN AUDIT TEAMS**

With the new Revenue Recognition and Lease Accounting standards taking effect soon, many audit departments have been bolstering their team’s skills with targeted, technical trainings. However, technical training alone may not be sufficient to build balanced audit teams, as the team members themselves may have development needs beyond audit and testing procedures. After all, is it not the goal of every team manager to leverage everyone’s skills and natural talents to maximize their chances for success?

We’ll first look at the need for performing a skills assessment, to determine a baseline between team members. Audit teams must continually review and revise the links between skills, performance, and training programs. To identify the most important skills for team members’ roles and to understand what skills they currently lack, the manager should consider conducting a skills gap analysis. Picking the right metrics is the key to creating real value from training. Often, organizations will assess their current performance against industry benchmarks:

- What is the typical number of testing hours for an organization our size?
- What is the typical count of controls for an organization our size?
- What are the top three training courses being discussed by the Big 4?
However, publicly shared metrics may not be relevant for your specific organization and culture. Each audit team should consider measuring the impact of its training programs through non-traditional metrics, such as:

- Number of meetings (and follow-up meetings) performed with a process owner?
- The average number of days to receive a PBC item?
- Evaluating the number of hours each auditor spends on testing a control?

These metrics can be useful in determining where audit staff are struggling to build rapport with their process owners, or having difficulty in completing a test due to the inherent complexity of the environment. Inexperienced managers take for granted the effort each auditor must face when working with a busy control owner, and end up spending unnecessary hours calming people’s nerves or rectifying the team members mistakes.

Regardless of how technical or complex a process may be to the auditor, professionalism and emotional intelligence are critical areas each auditor can further develop. More attention should be paid to human interactions, improved communication and etiquette, bridging cultural differences and geographies, and building empathy with the audit audience. A best practice for audit teams pursuing better relationships with business units and process owners is training their managers to provide real-time coaching and feedback sessions, and sharing examples of ideal client interactions. Junior auditors need examples and lessons gathered from real-life experiences, not just best practices shared in a training video.

The following is a list of “soft skill” topics each auditor should incorporate into their testing routine. Mastering these topics can lead to better relationships with the business, which can lead to quicker handover of evidence and more meaningful conversations, especially during walkthrough procedures.

- Effective Critical Thinking
- Communication and Negotiation Skills
- Interviewing Techniques
- Leadership Skills
- Relationships and Interpersonal Skills
- Succession Planning
- Understanding and Applying Emotional Intelligence

**STRATEGY 3 - LEVERAGE TECHNOLOGY**

There are two clear technology components of every audit function: Microsoft Excel and Email. Microsoft Excel was released in 1987 (Happy 30th Birthday, Excel!). Throughout this time, the lowly spreadsheet has evolved to be more than just a bookkeeping tool. Over time the simple spreadsheet has morphed into a workflow staple, due in part to its ability to link data across different documents and automate basic workflow tasks. Accordingly, modern audit projects require more attributes and details about a control than in years past. Whether it’s documenting the completeness and accuracy of evidence, or validating the integrity of a key report, testing procedures have evolved beyond simple attribute ticking and tying. The modern spreadsheet can handle this robust testing process; but, the spreadsheet lacks speed, efficiency, and consistency.

However, to keep up with the ever-growing list of testing requirements, audit teams have accepted MS Excel to be the cornerstone to their testing program. And, with the ever-increasing number of spreadsheets floating through the organization, shared network folders or a cloud-based collaboration tools have been introduced to help coordinate the information while organizing the staff.

While this approach is manageable for teams of 3 or less, once audit teams exceed 3-4 people, version control issues
become dramatically more complicated and much more time consuming to resolve. From past experiences as an audit manager, if one member of the team fails to make a timely edit or forgot to make updates across all test sheets, the downstream ripple effect would cost managers hours and hours of cleanup. Unfortunately, this painstaking cleanup process often goes unreported to the client and the budget is sacrificed.

So, why are teams still leveraging the spreadsheet? The answer: familiarity.

Given the complex nature of modern audit programs, audit data points often have a many-to-many relationship when it comes to risk and control mapping. Some examples include: risks that appear across multiple processes or business units, audit issues that impact multiple controls or processes, and COSO principles mapping to many controls.

The solution is to leverage an underlying database as the foundation of the audit program. Audit software constructed upon purpose-built database structures can allow auditors to quickly pull or push information to and from a database, and have those results cascade throughout the entire audit program instantly. This is far more efficient than the spreadsheets-based environment, where a control testing update would require making edits across several standalone spreadsheet files. In addition, for annual audit results to be used year over year, a spreadsheet cannot handle the large volumes of data. No amount of spreadsheet automation can compete with the speed, accuracy, and scalability of a database solution.

The good news is, as the industry has evolved, technological innovators have risen to the occasion. It is up to audit teams to understand their pain points, prioritize their organization’s needs, then carefully research the right solution to meet those needs.

CONCLUSION, WRAP-UP

The success of SOX in re-establishing investor confidence and improving internal control over financial reporting speaks to its lasting importance. There are high expectations and rules mandated year over year by regulatory bodies and external auditors. Now, the public and shareholders have come to expect a solid controls environment with every public company.

These high expectations have made quality, in-depth testing no longer an option - it’s a requirement for a company to operate successfully. However, striking that balance between quality testing vs. limited budget and staffing remains a puzzle every organization must solve.

As mentioned earlier, by reducing the total count of controls and focusing only on high risk, high impact areas of the business, audit teams can cut down on unnecessary testing procedures and unburden themselves from the monotony of repeating the same process year over year.

Secondly, training should go beyond regulatory and technical audit topics. Each auditor is a liaison to the business, and an ambassador for the compliance function within your organization. Train them, mentor them, and help them become a welcome member of the organization. The return on investment will go well beyond the results of a controls test.

Finally, audit technology has caught up with the demands of the audit world. However, there is an over-saturation of older, over-engineered solutions in the market. Be aware of the technology and its underlying platform. A well-made solution increases the opportunity to minimize unnecessary administrative tasks and can automate repetitive updates which are of little value to the company.

Consider the three strategies outlined, and help your audit teams unburden themselves from unnecessary expectations and focus on delivering the most valuable and cost-effective results to their organization.
Eight Things Every Internal Auditor Should Know About Sarbanes–Oxley

By Matt Kelly

In a certain sense, Sarbanes-Oxley compliance is an annual rite of passage, akin to the arrival of spring or the fall television season. The exact experience changes from year to year, but it always happens.

Indeed, for SOX compliance professionals under the age of 35 or so, it might seem like documenting and testing of internal controls is all there is to SOX compliance. Nothing could be further from the truth.

So as SOX turns 15 this fall, let’s widen the lens to capture what SOX is really about: its history, its goals, and the most important points to remember for an effective SOX compliance experience.

SOX was about more than Section 404 and ICFR. Congress enacted the Sarbanes-Oxley Act in 2002, amid deep suspicion that corporations, and the financial statements they published, could not be trusted. The goal of SOX was to place accountability for corporate behavior with the highest levels of the business: the board, the CEO, and the CFO.

Hence the law has other objectives well beyond Section 404. Among them: whistleblower systems for anonymous reporting of possible fraud (Section 301); CEO and CFO certifications that all financial disclosures are accurate (Section 302); prompt disclosure of material changes in a company’s financial situation (Section 409); and penalties for retaliation against whistleblowers (Section 806).

All those sections, and others, work to the overall goal of more reliable corporate financial statements, through the mechanism of greater accountability on senior corporate executives and board directors.

Original estimates for SOX compliance costs were wildly off. In 2003, officials from the Securities and Exchange Commission estimated that the annual cost of SOX compliance would
average about $92,000 per company. They were wrong: SOX compliance costs have been far higher. According to Protiviti’s 2017 Sarbanes-Oxley compliance survey, annual compliance costs now average $700,000 for non-accelerated filers, $1.14 million for large accelerated filers.

The repercussions of that first misjudgment about cost continue to this day. Anti-SOX critics have used it to push for amendments to the law, such as a section of Dodd-Frank Act of 2010 that exempted non-accelerated filers from Section 404(b), the annual audit of internal control over financial reporting. Some lawmakers want to expand that Section 404(b) exemption to more companies yet.

Current SEC leadership, meanwhile, wants to reduce compliance requirements; altering how the Public Company Accounting Oversight Board applies auditing standards around ICFR is one possibility. The SEC held a hearing on Section 404(b) burdens as recently as Sept. 13.

All the anti-SOX discourse heard today (and the SOX compliance community will hear much more in months to come) springs from the premise that initial estimates of compliance costs were low, and that the benefits aren’t worth the costs incurred.

SOX has worked. If the principal goal of SOX was to make financial statements more reliable, that has happened. According to analysis from Audit Analytics, the total number of restatements for U.S. filers went from 1,853 in 2006 to 671 in 2016. As a percentage of the total filer population, restatements fell from 11.9 percent to 6.8 percent.

Key characteristics of financial restatements have improved, as well. Average number of days restated; average time to complete the restatement; average size of the restatement in dollar terms, average number of issues cited in the restatement—all have fallen precipitously from the mid-2000s, when companies first began compliance with Sections 302 and 404, to today.

Other recent research suggests that strong internal controls also reduce the risk of accounting fraud. A study from the University of Texas at Austin found that companies disclosing fraud were 80 to 90 percent more likely to have previously disclosed material weaknesses; 30 percent of the companies studied also had prior auditor warnings of material weakness in internal control.

Internal control weaknesses come in three sizes: deficiency, significant deficiency, and material weakness. The standard definitions for each type of internal control weakness are clear:

- A deficiency exists when the design or operation of an internal control doesn’t allow employees to prevent or detect misstatements on a timely basis.
- A significant deficiency is a deficiency serious enough to warrant attention from senior executives who oversee financial reporting.
- A material weakness is one or more deficiencies so severe that there is reasonable chance of a material misstatement of financial data that won’t be caught promptly.

Understanding the nuances of those three definitions is crucial. For example, a company only needs to disclose material weaknesses to investors, not significant deficiencies. But if a significant deficiency contributes to that material weakness, then the company “must disclose the material weakness and, to the extent material to an understanding of the disclosure, the nature of the significant deficiencies.” (Per the SEC’s guidance on management’s report on internal control.)

What’s more, while significant deficiencies don’t need to be disclosed to investors, an auditor aware of those deficiencies must communicate them to the audit committee.

Communications among audit firm, audit committee, and management are critical. The requirement that auditors bring
significant deficiencies to the attention of the audit committee underlines a crucial point: clear communication among all three is paramount.

For example, SOX compliance officers must talk with external auditors regularly to determine which controls should be in scope for an ICFR audit, and to what extent the audit firm will rely on work performed by the internal SOX compliance team. Those decisions have direct consequence for how much time and money the company will spend on SOX compliance.

Meanwhile, management and audit firms will both talk to the audit committee about the company’s financial reporting. Differences of opinion can arise, but they should be truly that: questions about judgment, rather than misunderstandings about issues.

If management and auditor disagree about whether a specific deficiency is significant, the audit committee could ultimately referee that dispute. On the other hand, if they disagree about what the definition of a significant deficiency should be for a certain control, that requires more discussion between SOX compliance team and external auditor.

Cloud computing has changed SOX compliance enormously. The rise of outsourced service providers (OSPs) is one of the most significant changes to the business environment since SOX was enacted in 2002. OSPs, delivering data processing and other business functions via “the cloud,” affect SOX compliance in two major ways.

First, cloud computing increases a company’s concerns about access control and oversight of third parties. More outsiders might work with your organization’s financial data, or financial applications. That requires more attention to your own controls, and more careful risk assessment and testing of the OSP’s access controls.

Hence we saw the arrival of more sophisticated SOC 2 audits in 2011: audits of an OSP’s security controls. SOX compliance officers must ensure those audits are scoped correctly, to provide useful information to you.

The more you automate, the better off you are. Manual processes—from testing controls, to operating controls, to certifying control effectiveness, to collecting documentation, and much more—are the bane of SOX compliance. They allow more chance for error and loss of version control. Hence the strategy of automating controls and processes has become so crucial.

For example, companies might have a control that works in two phases, where Employee A must certify his component’s effectiveness before Employee B certifies hers. Done manually, this creates the risk that Employee B might certify her component before Employee A (emailing an attestation, say, while Employee A is on vacation), and a SOX compliance director doesn’t catch the discrepancy.

An automated approach might build logic into a certification and documentation system: a database of Web-enabled forms, so Employee B can’t certify her component of the control until Employee A completes his certification first.

Improvements like that, scaled up to the vast range of control activities most companies perform, is what automation seeks to deliver. That concept—“How can we simplify our internal control processes to reduce the opportunity for error?”—should be a guiding principle for all a company’s efforts to rationalize and reduce the number of key controls.

SOX compliance brings more benefit than a clean audit report. In the same way that SOX was about more than effective internal control over financial reporting, SOX compliance can deliver more benefit than a clean audit report and reliable financial results.
As noted above, SOX compliance correlates to reduced risk of fraud and financial errors. But consider: how many workplace harassment issues came to management’s attention, thanks to whistleblower hotlines created by SOX? How many cybersecurity breaches never happened, thanks to more attention to IT general controls? (Not enough, but the point is clear.) Academic studies have found SOX compliance—specifically Section 404(b)’s outside audit of ICFR—contribute to higher market valuations and stronger credit ratings, which in turn cut the cost of a company’s capital when seeking debt in the markets.

The point is that SOX compliance does serve a purpose. While the mechanics of compliance may be imperfect, the purpose itself is worthwhile, and the Sarbanes-Oxley Act achieves what lawmakers want it to do.

Reliance on financial statements, interdependence of risk, services delivered over the cloud—none of that is receding. So compliance officers should prepare for an even more interesting ride as we enter the next 15 years of SOX.
As we noted in the introduction, the central premise of SOX is establishing stronger control over financial processes to reduce the risk of fraud or error. Regardless of what regulatory or economic changes might come in the future, the importance of that premise is not going to recede. Boards and investors will never start to care less about the reliability of financial statements.

What does that prime fact mean for SOX compliance professionals? Several points.

First, conversations among stakeholders in the compliance process will be critical, to get the process right. For example, the rise of cloud computing services has profound implications for SOX compliance. That means closer conversations with the IT department and CFO about what types of cloud services the enterprise wants to use; and closer conversations with audit firms about what controls will be in scope for an ICFR audit in that world, where your modern IT environment looks radically different than what you used in, say, 2008.

Second, despite the challenges around cloud computing, modern technology is still your salvation. Most service providers can now provide their service—whatever it is; from audit management to cybersecurity to monitoring key risk metrics—better than your own organization. Your future IT landscape is likely to be a collection of cloud services working together, each performing specific tasks however you want them to perform.

Third, in a world where technology can do whatever you want it to do, you need to know what you want to do. As always, that means a strong risk assessment, tied to clearly stated business objectives, is essential. A business can't leverage SOX risk assessment practices for enterprise risk management, if the enterprise isn't clear on what its objectives and risks are. You cannot rationalize and reduce key controls if business processes change constantly.

All three points were true from the first years of SOX compliance 15 years ago. Advances since then have simply amplified their importance: more conversation among stakeholders; better use of technology; clearer insight into objectives and risks. Only then can you keep SOX compliance as an efficient and useful exercise, even as organizations march into the next 15 years and beyond.
Company Overview

SOXHUB helps organizations streamline and manage their SOX and internal controls program and free up resource hours for more value-added activities. We offer a full suite of audit management solutions for SOX management, ERM, operational audits and workflow management. Find out why clients from Fortune 50 companies to pre-IPO companies choose SOXHUB.

Learn more at www.soxhub.com