

Automating Sarbanes-Oxley
Compliance Testing for SAP® Applications

**A Guide to Cost and Time Efficiencies
for Annual SOX Compliance Initiatives**



Background

The Sarbanes-Oxley Act of 2002 changed the way publicly held companies manage and, more importantly, control their business. For most companies, the most costly aspect of the legislation is Section 404, which includes the requirement for both internal management and an external auditor to report on the adequacy of the companies' internal controls over financial reporting. Section 404 requires companies to identify, implement, document and test the controls that manage critical risk over their financial processes. An FEI 2007 study indicated that, for 168 companies with average revenues of \$4.7 billion, the average compliance costs were \$1.7 million or 0.036% of revenue.* This is down from the results reported in 2006, which indicated an average cost of \$2.9 million or 0.43% of revenue.

Sarbanes-Oxley 404 compliance costs also represent a "tax" on inefficiency, where the cost for managing and testing compliance is significantly higher if the company has decentralized versus centralized operations and systems. The FEI survey referenced above indicated average compliance costs for decentralized companies to be \$1.9 million, while comparable sized centralized company costs were \$1.3 million. Costs of evaluating manual control procedures were also reduced through use of system or application controls.

To achieve the optimal level of cost and time efficiency related to SOX compliance, companies need to leverage their application systems in order to map their existing manual SOX controls to capabilities or controls that are built and included within these applications. By doing this, companies can then take maximum advantage of automated tools that both automate testing and automated the generation of documentation associated with that testing.

This white paper provides an overview of the compliance automation opportunity, how to validate the time and cost savings associated with this approach and the process for implementing an optimal automated compliance environment.

* [footnote FEI source – Davoll is working on this].

The Compliance Automation Opportunity

Depending on the size and complexity of the organization, the number of SOX controls can range from 50-250, or more. The average number of hours to manually test and document the results of a single SOX control is approximately 4-8 hours and sometimes more, based on complexity. The documentation of test results for SOX controls requires detail and precision since they will be reviewed and audited by both internal and external audit teams. Accurate and complete work papers are critical.

Each control must be tested with two considerations in mind:

- **The Test of Design (TOD).** The test addressed here must confirm that the design of the control is still in place as defined to control the business risk as documented.
- **The Test of Effectiveness (TOE).** This test must confirm whether the control works effectively based on its intent or design, as defined above in TOD.

Evidence of both TOD and TOE must be shown for each control annually to prove the control continues to work effectively to address the defined financial risks. Because external auditors cannot rely on testing by the business owners, all critical controls, as defined by the auditors, must be retested by the external audit team. This cost comes back to the company in terms of annual audit fees.

Some companies use a third party to assist in the testing of key controls. Although the costs associated with this work must be included in the overall cost of managing the SOX effort, often the external auditors will rely on this independent work and not require additional external audit team testing. It can also significantly reduce the time spent by the business teams to execute this testing. With this approach, however, the business is required to review and approve all test results, and in many cases the business does not have expertise in this type of testing and is therefore inefficient in getting the test work done.

An automated testing solution, on the other hand, such as Worksoft Certify®, offers the time-saving benefits of the third-party testing approach along with thorough and complete work paper documentation in a timely manner, without requiring specialized skill-sets and the external costs.

Establishing the Business Case for Automation

To quantify the cost and time savings associated with an automation approach, there are specific pieces of information that need to be gathered. While the majority will be quantitative, some of the testing considerations may not have been tracked and will therefore be qualitative. Both are critical to the final analysis, so leverage both business experience and your internal SOX leadership team to obtain the information needed.

First, gather the facts. In many companies, this information is readily available from the team who manages Sarbanes-Oxley compliance within the organization.

- ▶ **How many SOX controls does the company use to manage their Sarbanes-Oxley compliance effort on an annual basis?**
- ▶ **Divide the controls by manual and application or system controls. Note which system is used to manage each application control.**
- ▶ **Who currently does the testing and documentation of each control? Record the results with each control. Note if groups of controls are tested by one individual within a functional area or whether the work is spread across a large group of business owners.**
- ▶ **Who owns the control and signs off on the testing and results? This typically is a manager or director of the functional area. Note the business owner for each control.**
- ▶ **Is any third party used to test some or all of the compliance controls? Which group of controls do they test? What are the fees associated with their work? If you can break the cost down by control, this is ideal. Record the results against the control base involved.**
- ▶ **Working with internal SOX leadership, define the critical controls that are re-tested by the external audit team and create an estimate of the fees* specifically associated with this work.**

**Note that in most cases, the actual fees associated with this portion of the external audit work may not be broken out as a separate line item, so work with your internal finance team to determine a reasonable estimate.*

Now that you have the control baseline, obtain from the business users an estimate of the hours it currently takes for them to:

- ▶ Execute the control tests, both TOD and TOE.
- ▶ Record and document the results, including the detailed work papers.
- ▶ Review and approve the results (work of business owner).
- ▶ Identify the additional hours spent by both the internal audit team and/or the SOX leadership team to review and monitor the compliance testing effort.
- ▶ Align those hours with each control to enable further detail of time and cost savings as automation savings baseline is further refined.

Using the controls worksheet, calculate the internal hours currently used to execute testing of the company's SOX controls and the identified external costs associated with this work (third party and external auditors). If the company wants to assign a cost to the time spent by internal resources, assign those rates to the hours defined. In either case, you now have an initial baseline for defining the cost and time savings associated with automating your compliance effort.

Establishing Goals to Optimize Your ROI Benefits by Automating Your SOX Compliance Testing

The initial baseline establishes the total group of controls that can be considered for automation; however, some portion will continue to be manually tested due to the nature of the control. The strategic direction should be to automate as many controls as possible, keeping the following goals and benefits in mind:

Goal	Goal Description	Associated Benefit
Goal 1	Significantly reduce the person hours associated with testing by automating the controls testing and work paper creation.	The hours associated with every control that is automated is reduced down to only the business owner approval hours; typically a reduction of 8-12 person hours per control.
Goal 2	Eliminate the external costs associated with third-party testing.	By automating the controls work done by third-party providers, you eliminate the external costs without introducing more work back on the business. Reliance based on automation should be retained for external audit consideration.*
Goal 3	Eliminate the need for additional effort in creating manual work paper documentation by using Worksoft Certify® for automated test reporting capabilities.	Worksoft Certify, an automated testing solution, automatically creates work papers, eliminating the need for extra effort in preparing audit-ready documentation.
Goal 4	Automate the assessment of year-to-year change related to controls.	By assessing what has changed and what has not, some control testing can potentially be distributed over a longer period of years, versus testing all controls every year.*
Goal 5	Reduce the overall time required to execute annual SOX control testing.	Depending on the number of controls, it is reasonable to target completion of all testing and documentation within a one week period versus multiple weeks to months of effort.
Goal 6	Automate the management, monitoring, and communication of controls testing and results with online dashboards and metrics.	Automated tracking of the testing reduces the need to manually track the progress, execution, and results of the testing. Real-time visibility to test issues enables quicker resolution and retesting to obtain final, positive results.

* External auditor review and approval required

Procedure for Building and Executing Your Compliance Testing

The first step in building your automated compliance test baseline is to define what is appropriate to build. Use the following table to help define an automated baseline:

Step Number	Step Name	Step Procedure
1	Gather	<ul style="list-style-type: none"> Working with SOX management, obtain list of all controls — manual and system — and related test documentation
2	Analyze	<ul style="list-style-type: none"> Working with relevant business lead, assess each control to determine how it can be automated, including current manual controls Engage subject matter experts (technical and business) to answer any questions regarding how control is used and how automation can be applied
3	Prioritize & Plan	<ul style="list-style-type: none"> Working with SOX management and external auditor, prioritize those controls that external audit relies on most heavily during their review Working with audit schedules, build plan to automate controls in support of SOX testing time frames

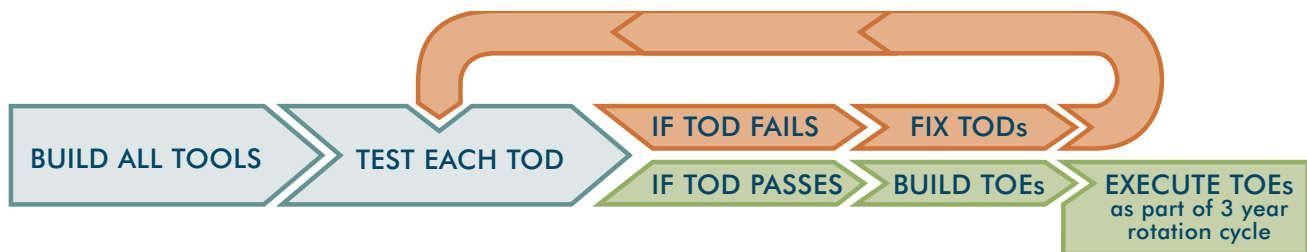
Based on the prioritized list of controls, and using the manual version of each test, first build the Test of Design (TOD) for each control using Worksoft Certify®. There are two reasons for doing this:

- 1.** The TOD forms the baseline of testing for each control. By building the TOD first, which is quick and straightforward, you can establish the foundation for all your Tests of Effectiveness or TOEs.
- 2.** In executing the TODs, you can quickly determine if there have been any changes in the system that require changes to the TOD or further documentation. Specifically, if you run the TOD and get a failure, you know that either something has changed in your system, which means the control needs to be reviewed or modified, or you used bad data, which means that the business needs to get involved and evaluate why this occurred.

In either case, by building and running the TODs first, you can quickly establish your automated test baseline and know what to adjust before you complete your Tests of Effectiveness or TOEs.

There is an additional reason to run the TODs first. Based on approval from your external auditors, you may be able to further condense your testing scope. If the test of your TODs shows that there has been no change in your system since last year, with external auditor approval, you may be able to do 3 year rotational testing of some of the controls, so that you reduce the total scope of TOE testing required each year.

The diagram below explains this process.



There are significant time and cost savings associated with this approach. However, make sure you work with your internal SOX leadership and your external auditor as you plan and implement this process to get their complete buy in and sign off.

Real Life Example of Automated Build and Time and Cost Savings

Let's take a look at a typical SOX control for an SAP application and compare the time and cost savings using this approach. The audit test description and associated control are as follows:

- **SOX DEFINED TEST (AUDIT TEST DESCRIPTION):** Validate that field status settings are configured to enforce key fields as required entry when entering a purchase order in the SAP application.
- **ASSOCIATED CONTROL (CONTROL ACTIVITY):** The SAP® application is configured to require key fields (price, cost object, etc.) when entering a purchase order in the system.

The manual version of the Test of Design (TOD) will consist of these components:

- The screen layout is formed by a combination of the transaction code, activity, document type, and item category/document category. Each of these has a corresponding entry in the Field Selection column.
- Creating a standard NB purchase order for a standard item would have the following field selections:
 - AKTH - Activity
 - ME21N - Transaction
 - NBF - Document Type
 - PTOF - Item category/Document category
- The standard SAP® application implements Fields configured as 'required entry' over Fields configured as 'optional entry' (AKTH) when entering a purchase order.

In comparing the manual time to run this Test of Design versus the time to execute this test once automated (using Worksoft Certify®), the following statistics are produced:

Type of Test	Number of Screens/ Fields to Validate	Test Execution Time	Time to Document Test Results
Manual Testing	75	4 hours	8 hours
Automated Testing	75	10 minutes	0 hours – documentation automatically generated

Key considerations:

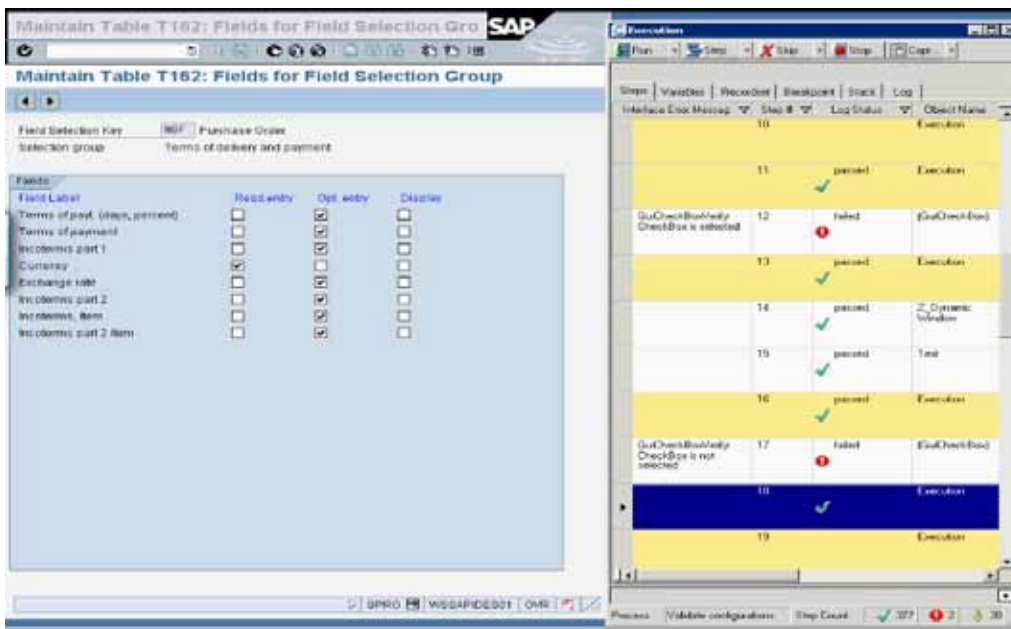
- If this test is executed manually by the business, may still need to be retested by external auditor.
- If this is done by third party, the company will incur the cost of testing and documentation – must be repeated each year.
- With automation, there is no business intervention in running the tests and documenting the findings.
- With automation, one person can execute both tests and results, which can then be reviewed/confirmed with business and auditors

Equivalent, comparable results also occur with the Test of Effectiveness (TOE) for this control. Comparing the manual time to run this TOE versus the time to execute this test once automated (using Worksoft Certify®), the following statistics are produced:

Type of Test	Number of Screens/Fields to Validate	Test Execution Time	Time to Document Test Results
Manual Testing	75	4 hours	4 hours
Automated Testing	75	10 minutes	0 hours – documentation automatically generated

When Failures Occur

Sometimes, tests will fail. However, the management of failures is much more efficient with the use of Worksoft Certify®. Here’s an example:



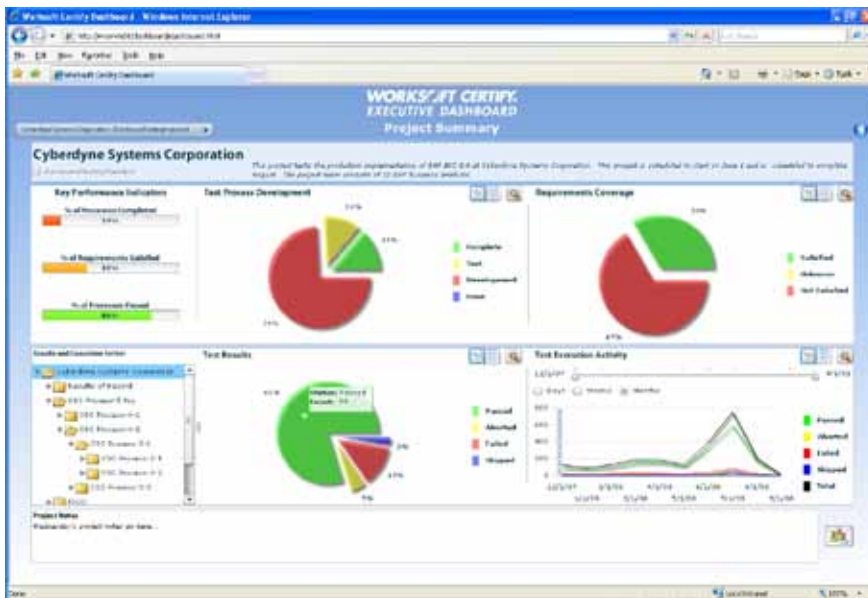
In this example, there was not accurate data to complete the required fields and the test failed. Worksoft Certify’s automated reporting tools, both the tester and the developer can quickly locate exactly where the test failed and what caused the test to fail. In some cases, it is as simple as providing good data, but in other cases, a developer may need to fix a problem in the system.

Key Considerations:

- With automated testing, you can configure the test to stop at any failure and document which step in the process caused the failure.
- This documentation can then be provided to the developers to fix and prepare for retest.
- The automated test can then be pointed:
 - First to the test environment to validate.
 - Second, to the production environment for further validation if fix passes initial test.
- All this repeated testing can be executed by one person with all documentation fully detailed.

Managing Automated Compliance Testing

Keeping all interested compliance members aware of the testing process and results is critical to long-term management and buy-in. The Worksoft Certify Executive Dashboard™ solution provides all parties clear and concise views of the testing process and the results in real-time and streamlines the management and monitoring requirements. Please see an example below.



Conclusion — The Benefits of Automating Your Compliance Testing

The regulatory requirements for continually validating that your organization is well controlled and managed may not change. However, the means by which your organization manages, monitors and reports on your compliance can be optimized and streamlined by taking an automated approach. The benefits are many. The following highlights some of the critical results and savings you can achieve:

- ▶ You can quickly assess your production environment and determine and validate what has remained the same and what has changed.
- ▶ You can use expedited testing, leveraging automated TODs for all application controls, to further define what needs extended testing/validation.
- ▶ All your documentation for both TODs and TOEs is automatically created as part of the Worksoft Certify® test runs; no need for additional documentation.
- ▶ The results of all your automated test efforts are presented in an easily readable format that both internal and external audit/SOX teams can use and review.
- ▶ One person can execute all automated testing, significantly reducing the time and effort normally required by both business and audit teams to obtain results.
- ▶ Because these tests need to run against your production environment, by using the automated test build, you can specifically control what is executed and when it is stopped. This eliminates any potential opportunity of executing more than what's needed or planned.
- ▶ Per external audit agreement, the external audit team can rely on these results without third party intervention, thereby eliminating third-party costs and significantly reducing external audit costs associated with executing these tests manually. In many cases, you will only need to review results versus re-executing critical application control tests.

How to Take the Next Step towards Automating Your SAP Compliance Testing

To learn more about how to automate compliance testing for your SAP® applications or to learn more about Worksoft Certify, please contact Worksoft at (214) 239-0400 or visit www.worksoft.com.

