



# How Perforce Can Help with Sarbanes-Oxley Compliance



**C. Thomas Tyler**

Chief Technology Officer, The Go To Group, Inc.  
In collaboration with Perforce Software



## Perforce and Sarbanes-Oxley

The Sarbanes-Oxley Act requires accountability in the management of systems that affect financial reporting. Perforce delivers key features necessary to comply with the law, such as access control, strong accountability, and policy enforcement tools. Better still, Perforce provides an efficient infrastructure for an automation-based approach to compliance that yields enhanced productivity—a nice side benefit.

### Sarbanes-Oxley in a Nutshell

The Sarbanes-Oxley Act of 2002 is legislation aimed at improving investor confidence in the American financial trading system. The Act promotes new standards for financial reporting for public companies, and sets up a policing mechanism to ensure those standards are adhered to.

The big news for information technology is Section 404 of the Act, titled “Management Assessment Of Internal Controls.” Section 404 effectively expands the scope of financial report auditing to include internal controls. Among other things, that involves IT systems and processes that produce financial reports. The Act requires that management of public companies attest to the effectiveness of those systems, and that registered public accounting firms audit the internal controls, then append their own independent assessments of the effectiveness of those controls.

To form an opinion about the effectiveness of IT systems, financial reporting auditors are more technically savvy about the management and operation of IT systems than ever before. They’re asking tough questions: How can changes made to your financial reporting software be audited? What Software Configuration Management systems are in place, and are they used for

all systems that significantly affect financial reports? What access controls are in place to prevent unauthorized personnel from modifying financial reporting systems? What is your change management workflow?

For those in the software development world who have been involved in efforts to improve the software development process, these are familiar questions. Sarbanes-Oxley simply forces public companies to answer them, at least with regard to those systems contributing significantly to financial reporting.

### What You Need to Know About Sarbanes-Oxley Compliance

If you work for a public company, you need to know that following established best practices for development and maintenance of certain software systems—those that can significantly impact financial reporting—is now required by law. Audits of financial reports go far deeper than just reviewing the financial reports. They go into the heart of IT systems that produce those reports. The law makes it clear that corporate executives are responsible for attesting to the quality of the controls that produce their financial reports, and that statements they make must be auditable. Further, auditors from public accounting firms are responsible

for making their own independent assessments of the effectiveness of the company's controls.

How do auditors determine what's effective? It turns out they have some good ideas about how to ensure that IT systems are managed effectively, because best practices have been established, have evolved, and have matured within the software world for decades.

Established disciplines such as configuration management and change management have evolved to help answer the questions auditors love to ask, such as "Who changed what?", "When did they do it?", and "Why?" With Sarbanes-Oxley, you can't get away with answering those questions just once during the audit.

You have to show how the systems you have in place can answer those questions at any time. This is reinforced by Section 409 of the Sarbanes-Oxley Act, titled "Real Time Issuer Disclosures." Thus, there's a natural tendency for auditors to favor solutions involving extensive automation.

Prior to Sarbanes-Oxley, audits focused primarily on the resulting financial reports, and rarely on internal controls surrounding the systems companies used to generate those reports. When audits of systems

did occur, the standards used to evaluate a company's systems weren't consistent. With Sarbanes-Oxley, the efforts of public auditing firms are now coordinated by the Public Company Accounting Oversight Board, or PCAOB (<http://www.pcaob.org>), which was chartered by the law. The PCAOB is responsible for establishing and adopting standards used for auditing internal

controls of public companies. The Board ensures that internal controls of all public companies are audited against a common set of standards.

What are the auditors looking for from CIOs and IT managers? They're looking to make sure that systems used to produce financial reports follow industry best practices. Although the law doesn't explicitly define best practices, in practice auditors rely on established standards for measuring the

maturity of various processes. For example, if your organization has been "climbing the SEI scale,"<sup>1</sup> or working toward ISO 9001 certification, you'll be able to answer some of the auditors' initial questions quickly. Auditors consider a wide range of factors, such as the ability of your process to provide basic quality assurance, and the ability of your systems to assure that only authorized personnel have access, to name a few things.

Established disciplines such as configuration management and change management have evolved to help answer the questions auditors love to ask, such as "Who changed what?", "When did they do it?", "Who approved the change?", and "Why?" With Sarbanes-Oxley, you can't get away with answering those questions just once during the audit.

1. The "SEI scale" is an informal reference to the Software Engineering Institute's Capability Maturity Model.

### Prominent features that make Perforce particularly well suited to Sarbanes-Oxley compliance efforts

- Configuration management.
- Software Development Life Cycle (SDLC) support, including support for clear hand-offs and promotions. Promotions can involve anything represented as a file: source code; documents; and runtime environment files such as libraries, executables, images, and even large files such as CD images.
- Access controls and the ability to assign promotion authority to groups of authorized users.
- Audit trails for various activities.
- Ability to rollback changes.
- Change management for runtime environments.
- Document management and document promotion.
- Change review notification.
- Policy enforcement triggers.
- Integrated enhancement, bug, and issue tracking.
- Workflow process management support.

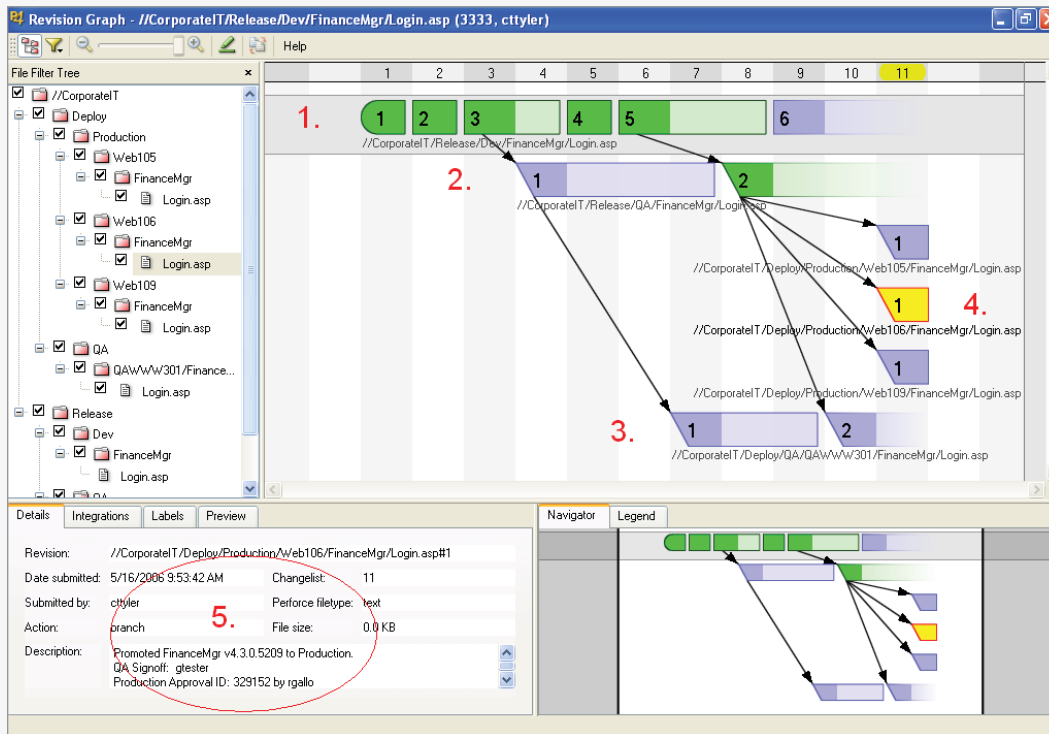
04

For example, take Configuration Management (CM) as a sample discipline. Within the software development world, CM (sometimes called SCM, for Software Configuration Management) is considered the foundation of any organized software development process. When you attempt to achieve any measure of quality for a software development process, CM infrastructure must be in place, just as surely as the computer network. For example, to climb only to Maturity Level 2 on the Software Engineering Institute's

capability level scale, CM is one of the key process areas that your organization needs to establish. When auditors are seeking to determine the effectiveness of internal controls, their job, and your audit, will go a lot easier if you can show that you have the basics, such as CM, under control. One word of caution: be wary of scope creep in your efforts to comply with Sarbanes-Oxley. The reality of modern public companies is that everyone depends extensively on IT to support financial reporting. The intent of Sarbanes-Oxley is to ensure that the IT systems used for financial reporting have effective controls that are designed and operated in such a way that they're reliable. The focus is on just those IT systems that can materially affect your financial reporting. Sarbanes-Oxley audits typically start with an assessment of just which systems and controls should be audited. The scope of a Sarbanes-Oxley audit is limited with regards to IT: it doesn't apply to your products or services, which can also rely extensively on IT. For reasons of efficiency, you might want all such systems to follow best practices, but that's going above and beyond what's required for Sarbanes-Oxley.

### Ways Perforce Helps with Compliance

Yes, Perforce can indeed help with compliance. In practice, Sarbanes-Oxley compliance projects often involve automation of internal controls. To that end, Perforce takes you much farther down the road to Sarbanes-Oxley compliance than traditional SCM systems. Perforce provides strong mechanisms to ensure compliance with established policies. Perforce's extremely efficient and robust architecture allows you to use it to manage much more than source code, extending the ability to



**Figure 1: Perforce managing runtime environments**

1. The Development Release Area is a “no humans allowed” area, populated by automated build processes. Several builds are shown deposited here.
2. Selected builds were promoted to the QA Release Area.
3. Software from the QA Release Area was deployed to a runtime environment on the QAWWW301 machine.
4. The QA'd software was later deployed to Production runtime servers: Web105, Web106, and Web109.
5. You can see the details of when and where changes occurred. You can use Perforce policy enforcement mechanisms to ensure certain information is provided to allow a promotion, such as QA Signoff or an authorization ID.

support Sarbanes-Oxley objectives. And Perforce's powerful visualization tools can allow you to verify, for example, that software in Production first went to a QA environment.

Sarbanes-Oxley audits go broadly and deeply into IT systems involved in financial reporting—you need to do more than simply mark off a checkbox indicating that you have a CM system in place. Auditors take a “big picture” view, and they're responsible for making judgments about the overall effectiveness of your processes. A truly modern software production line that takes advantage of Perforce's extensive functionality goes a long way toward giving auditors the impression that you have everything in order—and that makes them less likely to feel the need to dig deeply and look for holes.

Perforce is an advanced SCM system, and provides a comprehensive foundation for a modern software production line. A Perforce-based software production line takes advantage of many aspects of Perforce's functionality that help support Sarbanes-Oxley objectives.

Because Perforce is particularly efficient at distribution of vast numbers of text and binary files, it's often used not only to manage source code, but also to handle distribution of files to live, runtime environments. The benefits of using an SCM system in this role are particularly apparent in light of Sarbanes-Oxley compliance, because the ability to answer

whodunit-type questions applies not just to the source code, but to actual updates to runtime environments, such as Production or QA. For example, Perforce can answer questions such as, “Who made updates to our Production systems today, who authorized them, and when did they occur?”

Figure 1 illustrates selected builds being promoted to new codelines. Note the details of when and where the changes occurred, as well as who made the changes and who authorized them.

SCM systems generally provide good accountability and audit trails, but their use has traditionally been relegated to source code control. Perforce is typically used for much more, due to

its efficiency at managing and incrementally distributing files. By extending its scope of control, Perforce becomes the heart of a runtime-environment management system, extending its strong controls and auditing capabilities far beyond the realm of source code.

Perforce also provides document management functionality. Various documents, such as standards, policies, and procedures manuals that affect financial reporting systems of a public company are within the scope of an internal controls audit. Perforce can provide a clear workflow for documents, segregating “in work” or “proposed” policy documents, for example, from “approved” documents. Using Perforce to manage documents provides a clear audit trail for documents as they move through that life cycle, and also provides whodunit information for those documents.

Perhaps the best thing about using Perforce to support your Sarbanes-Oxley compliance efforts is that the value added by using Perforce translates into a return on investment.

One interesting, often unexpected benefit of Sarbanes-Oxley compliance projects is the way they lead to enhanced communication, especially within larger organizations. For example, during this author's experience with Sarbanes-Oxley compliance projects, the first sign that an audit was in progress was a series of requests for Perforce licenses from business units that had never had a reason to interact previously.

Until that point, Perforce had been associated primarily with the software development business unit within the organization. It became clear that other business units had CM needs as well. What followed was a wider appreciation of the benefits of Perforce within the enterprise, as more and more systems were put into Perforce, some driven by Sarbanes-Oxley compliance, others after they learned of

the process benefits of doing so, such as process automation and rollback support. Technical experts from across organizational boundaries collaborated on compliance projects. The job got done, and the new relationships resulted in collateral benefit for the organization as a whole.

Perhaps the best thing about using Perforce to support your Sarbanes-Oxley compliance efforts is that the value added by using Perforce translates into a return on investment. Sarbanes-Oxley-driven compliance projects have yielded unexpected benefits in terms of increased efficiency through automation using Perforce. As mentioned earlier, auditors tend to favor internal controls that feature extensive automation, and Perforce is all about providing a foundation for a highly efficient automated software production line.

[www.perforce.com](http://www.perforce.com)



**North America**

Perforce Software Inc.  
2320 Blanding Ave  
Alameda, CA 94501  
USA  
Phone: +1 510.864.7400  
info@perforce.com

**Europe**

Perforce Software UK Ltd.  
West Forest Gate  
Wellington Road  
Wokingham  
Berkshire RG40 2AQ  
UK  
Phone: +44 (0) 845 345 0116  
uk@perforce.com

**Australia**

Perforce Software Pty. Ltd.  
Level 10, 100 Walker Street  
North Sydney  
NSW 2060  
AUSTRALIA  
Phone: +61 (0)2 8912-4600  
au@perforce.com