July 19, 2005

Software Configuration Management Tools Ease The Burden Of Compliance

by Carey Schwaber
with Christine Ferrusi Ross

EXECUTIVE SUMMARY

Process-centric software configuration management (SCM) solutions can help development shops achieve sustainable compliance with internal process improvement frameworks like CMMI and external regulatory requirements like Sarbanes-Oxley. Automated process enforcement, traceability, and auditing — all core capabilities of process-centric SCM solutions — enable shops with heavy compliance burdens to achieve significant efficiencies. But the extent of these efficiencies, and thus the return on investment for a process-centric SCM solution, varies with the number and import of internal controls. Different levels of controls are appropriate for different organizations, and most external regulatory requirements apply only to the development of particular kinds of applications.

PROCESS-CENTRIC SCM SOLUTIONS FACILITATE COMPLIANCE

Supporting changes in corporate governance to address regulations like Sarbanes-Oxley is the top priority for North American enterprises with more than 20,000 employees, and it's a priority for half of all North American enterprises.[1] But development shops must support internal process improvement and governance frameworks like CMMI, COBIT, ISO, ITIL, and Six Sigma in addition to external regulatory requirements like Sarbanes-Oxley, FDA regulations 21 CFR Part 11 and GxMP, and Basel II.[2] Development shops can use process-centric SCM solutions to help meet both internal and external compliance requirements, as these tools enable:

- **Process enforcement.** Compliance with internal and external regulations involves defining, implementing, and enforcing software development processes. When performed manually, these activities are time-consuming and error-prone; consequentially, firms often turn to tools that enable process automation. The process automation capabilities included in many SCM solutions help make process enforcement transparent, thereby enabling development shops to stay focused on their real mandate — delivering value to the business.

- **Traceability.** Regulatory requirements make traceability more than just an ideal: Enterprises now find that they both want and need to confirm that their systems actually do what they've been designed to do. Traceability enables firms to establish this by linking development artifacts like requirements, code, and test cases together and ensuring their correspondence. A solution that enforces change management policies — that is, any process-centric SCM solution, and particularly one that is part of a larger life-cycle management suite — is the nexus of any traceability effort.

- **Auditing.** Auditing capabilities have been part of SCM solutions for years, but regulatory requirements have made this functionality more important. While traceability verifies the proper

associations between development artifacts, auditing capabilities record their history, collecting information about who changed what, when, and why. The ability to implement controls is an important part of any compliance effort, but the ability to demonstrate the efficacy of the controls that are in place is even more important.

Not every shop that has adopted CMMI or every shop facing regulatory requirements needs the process automation, traceability, or auditing capabilities of a process-centric SCM system. It is possible to implement the necessary IT controls manually; the cost-effectiveness of doing so varies in proportion to the total number of controls. When it comes to regulatory requirements, enterprises should take a risk-based approach to compliance, instituting controls in proportion to their risk levels.[3] Development shops at firms grappling with Sarbanes-Oxley compliance should take note of the SEC's recent guidance, which states that the SEC does not expect testing of "general IT controls that do not pertain to financial reporting."[4]

RECOMMENDATIONS

SUPPORT FOR COMPLIANCE INITIATIVES VARIES BY SCM SOLUTION SEGMENT

Today's SCM market includes four distinct segments, each of which offers a different level of support for compliance initiatives.

- **Version control tools offer minimal compliance support.** Some source code control is certainly better than none, but development shops won't get much help meeting compliance requirements from tools like Concurrent Versions System (CVS), Microsoft Visual SourceSafe, and Subversion. Shops using version control tools will need to integrate them with complimentary tools in other life-cycle categories — for example, issue tracking tools and build tools.[5]
- **SCM tools include basic auditing capabilities.** SCM tools offer the basic ability to version groups of assets (i.e., configurations), which enables firms to better track the files that comprise particular releases. Build management capabilities are also included in most SCM tools. The combination of build management and configuration management allows companies to identify the exact makeup of apps in production — one of the most essential elements of regulatory compliance.
- **Process-centric SCM solutions enable process definition, implementation, and enforcement.** Solutions in this segment offer differing degrees of support for process design and implementation, but they all shine when it comes to process enforcement. Process-centric SCM solutions also enable some degree of traceability. For example, if they include integrated issue tracking, then developers' changes can be tagged as work performed in order to resolve particular issues.

- **Process-centric SCM as part of a life-cycle management suite enables full life-cycle traceability.** While process-centric SCM solutions can associate life-cycle artifacts like versioned objects with issues and requirements, SCM solutions that are part of full application life-cycle management suites take this a step further, extending traceability to design and testing artifacts. The more life-cycle tools that an SCM solution integrates with, the more parts of the development process it can positively affect.

ENDNOTES

[1] Twenty-seven percent of decision-makers at 868 North American enterprises indicated that supporting changes to corporate governance — like Sarbanes-Oxley — compliance is a critical priority, with the same percentage calling it a priority. But among the largest enterprises — those with 20,000 or more employees — changes to corporate governance will be the top priority. Thirty-eight percent of these enterprises named this as a critical initiative. See the December 15, 2004, Data Overview "2005 Enterprise IT Outlook."

[2] CMMI stands for Capability Maturity Model Integration, COBIT for Control Objectives for Information and related Technologies, ISO for International Standards Organization, and ITIL for IT Infrastructure Library. For more information, see the May 31, 2005, Trends "Stabilizing IT With Process Methodologies."

[3] IT organizations have always scrambled to align IT with the business, but now there's a new scramble going on — in the area of risk and compliance management. Faced with increasing pressure to demonstrate operational integrity, financial integrity, and regulatory compliance, large organizations have been building enterprise risk management (ERM) programs. In coordination with these enterprisewide initiatives, IT shops have been building their own processes to manage IT risk and compliance. See the March 15, 2005, Trends "Risk Management Catches On With IT."

[4] Organizations should adopt a top-down, risk-based approach to internal controls. Organizations have mistakenly approached Sarbanes-Oxley with a control checklist mindset. However, Sarbanes-Oxley cannot be approached as a checklist; as the SEC notes, there is no one-size-fits-all set of controls. The appropriate number of controls varies with risk, ranging from a few hundred to a few thousand. The SEC specifically recommends a risk-based approach to control identification. See the May 26, 2005, Quick Take "SEC Establishes Control Of SOX 404 Requirements."

[5] Sets of lightweight tools — point tools with open pathways for integration — represent an alternative to integrate tool suites. In the past, the primary alternatives to single-vendor suites were collections of individual point tools. Traditional point tools are typically larger in scope than lightweight tools and rarely integrate well with each other, relying instead on proprietary APIs, point integrations, and import/export pathways. A set of point tools that don't integrate with each other isn't a credible alternative to an integrated tool suite. What makes lightweight tools a compelling proposition is that each tool can be best-of-breed, while the tool set as a whole provides many of the benefits of tool integration that come from using a single tool suite. See the April 21, 2005, Trends "Lightweight Tool Sets Represent An Alternative To Integrated Tool Suites."