

Implementing, Enforcing, Documenting, and Auditing Compliance with AccuRev

Written by:



Damon B. Poole
AccuRev Chief Technology Officer

AccuRev

Executive Summary

There are many compliance standards and regulations in effect today, including Basel II, 21 CFR Part 11, COBIT, COSO, HIPAA, ISO 17799, ITIL, Sarbanes-Oxley, SAS 70, and others. Software Configuration Management (SCM) plays a key role in any compliance effort that involves software development. This technical whitepaper describes the specific features of AccuRev that support compliance and shows how the unique advantages of AccuRev can simplify your compliance efforts.

Fully Enforced Process - with AccuWorkflow™, you can implement a unified workflow which is shared by both your ITS system and your SCM system. That means that all users, whether they are managers, QA, or developers are all working within the same process and their activities are automatically coordinated.

Seamless Issue Tracking Integration Using Change Packages - change packages enable easy access to the progress of the issue and its current state can be seen via the source control system which is a more natural interface for developers.

Support for All Leading Issue Tracking Systems - out-of-the-box integrations including Atlassian Jira, Rational ClearQuest, MKS Integrity Manager, Bugzilla, Serena TeamTrack, and HP QualityCenter.

Separation of Duties - it is easy to configure AccuRev's groups, ACLs, and workflow to require that different users are responsible for initiating, assigning, completing, and reviewing changes.

Physical Security – AccuRev's TimeSafe append-only data model combined with its client/server architecture allows for physical security which provides a full and tamper proof audit trail.

Standards Based Authentication and Authorization – LDAP provisioning and authentication assures that users are automatically authorized for exactly the access that they need.

Extensible Controls - with fully configurable Workflow, Streams, and Access Control, AccuRev provides a wealth of compliance capabilities. If you need something beyond what is provided, you can use AccuRev's APIs and triggers to customize AccuRev to your exact needs.

Support for Audits - AccuRev's side-by-side StreamBrowser and Workflow diagram enable a visual self-documenting process which is instantly understandable without the need to create and update external documentation.

Keeping up with Change - AccuRev is designed around the philosophy that change is inevitable. In support of this philosophy, everything in AccuRev is configurable and flexible with good defaults to start from.

Fully Enforced Process

A key requirement of most compliance standards is to have a well defined and well documented Software Development Lifecycle (SDLC). It is far easier to define and document your process if it is directly supported by the software you use. AccuRev provides two complimentary capabilities for implementing your process: Streams and Workflow.

Most SCM systems use branches and labels to represent stages of development and releases. Branches and labels are set on a per-file basis and are not represented as high-level objects. These systems are oriented around files instead of process and workflow stages. Furthermore, file-oriented SCM systems do not support the ability to set relationships between branches and labels to support process and workflow. In a file-oriented system, process and workflow must be provided by the implementer via scripts and integration with an Issue Tracking System (ITS). Integration is a good thing, but if the process and workflow concepts only exist on the ITS side, it is difficult to leverage them on the SCM side.

AccuRev provides the functionality found in branches and labels via “streams.” Unlike branches and labels, streams allow you to create, visualize, and enforce your process model directly in the product.

Streams correspond directly to the code related workflow stages found in ITS systems. For instance, you can have streams for developers, teamwork, code review, integration, QA, and production which directly model the flow from development to production. This works great for stages that have code associated with them, but what about the stages that happen before and after coding?

Typically, the full SDLC is only represented in the ITS side of your development toolset. With AccuWorkflow™, you can implement a unified workflow which is shared by both your ITS system and your SCM system (see Figure 1). That means that all users, whether they are managers, QA, or developers are all working within the same process and their activities are automatically coordinated.

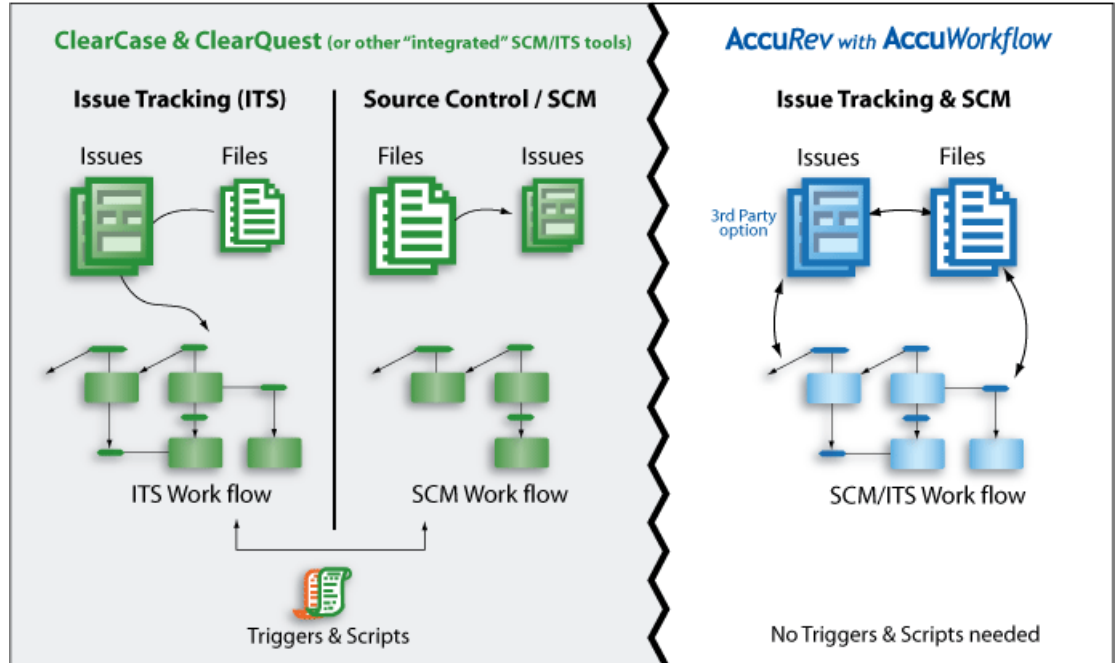


Figure 1: Unified Source Control and ITS Workflow

Having a unified process which both your ITS and SCM systems implement directly significantly reduces the need for manual process steps. The more automated your solution is, the more likely it is that your documented process is the process that is being followed. Automated process also provides enforcement. The more manual your process is, the more opportunities there are for users to make mistakes or subvert the process.

Automation of process enforcement also provides a benefit to developers. Instead of having to remember the exact steps to follow at each point in the process and worrying about making a mistake, the system will guide them through the process.

Seamless Issue Tracking Integration Using Change Packages

A significant part of your software development compliance efforts are focused on your issue tracking system. In order to be in compliance, all change requests must be tracked, and that requires the use of an Issue Tracking System (ITS). Furthermore, implementing a closed-loop system requires traceability from change request to actual change and back again. Traceability requires a tight integration between your Issue Tracking system and your SCM system.

AccuRev uses “change packages” for ITS integration. A change package represents a complete patch of all changes required to implement a particular change. It is a rollup of all of the changes that have been applied to resolve an issue including a complete audit trail of who made the changes, when they made the changes, and why they made the changes. Each change package is tied to an issue in the ITS. Unlike other integrations where all information about the changes associated with an issue are stored in the ITS, AccuRev stores all of the change information itself and the ITS information serves as a convenience to the ITS user. The advantage to using change packages is that the progress of the issue and its current state can be seen via the source control system which is a more natural interface for developers.

Support For All Leading Issue Tracking Systems

Only AccuRev provides out-of-the-box integrations with all of the leading Issue Tracking systems on the market today including Atlassian Jira, Rational ClearQuest, MKS Integrity Manager, Bugzilla, Serena TeamTrack, and HP QualityCenter. If we don't integrate with your system, we can work with you to provide it or you can use our integration SDK to do it yourself.

Separation of Duties

A key fraud prevention control is the separation of duties, also called segregation of duties. This is a well known financial, management, and legislative control which is now being applied to software development.

AccuRev has many capabilities that support the separation of duties. You can easily configure AccuRev's groups, ACLs, streams, and workflow to require that different users are responsible for initiating, assigning, completing, and reviewing changes. You can also set it up so that only certain users, or members of certain groups (roles) can perform these actions. This sharply reduces the chance that a change that will result in financial impropriety will make it into production.

Physical Security

One of the most effective forms of security is physical security. That is, putting your data repository in a physically secure location. This can then be secured using a lock, keypad, badge, biometric input device, or other physical security methods. In order for this to be practical, there must be a way for the users to access the repository at the application level using an access path that is guaranteed to be fully auditable.

AccuRev is TimeSafe®. It uses an append-only data model and a client server architecture. There are no commands in AccuRev which remove data, and all commands must be run via the client. All communication is via a single port which is configurable by the administrator. When combined with physically securing the AccuRev repository and only allowing AccuRev client software to connect to the machine, you automatically get a full and tamper proof audit trail of all Software Configuration Management (SCM) activities (see Figure 2). Even if somebody has been granted access that they should not have, you will be able to audit all of their activities. They will not be able to cover their tracks by removing the audit trail.

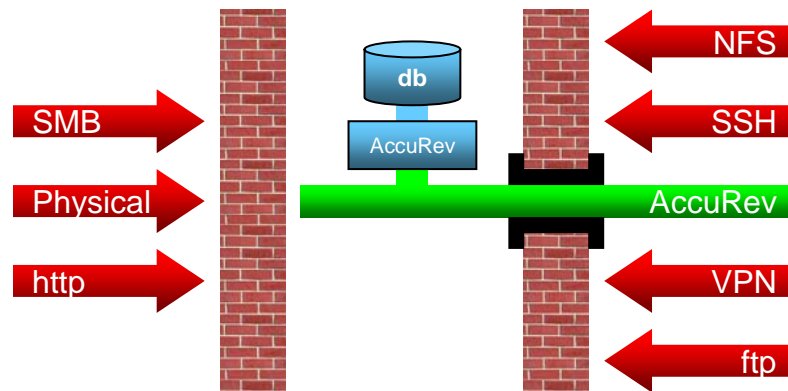


Figure 2: full and tamper proof audit trail of all SCM activities

SCM systems such as ClearCase® that rely on NFS are unable to provide physical security. In order for ClearCase to function, all users require full NFS access. Anyone that has NFS access can get full and unrestricted access to the ClearCase repositories, even if they are stored on machines that are under lock and key. Thus, all users of ClearCase have full and unrestricted access to the ClearCase repositories.

Even client server SCM systems other than AccuRev that allow physical security don't use an append-only data model, they provide operations which allow users to remove or overwrite data. Unless you know and have locked down all operations which remove or overwrite data, you cannot get a full audit trail.

Standards Based Authentication and Authorization

AccuRev supports LDAP integration for both provisioning and authentication. By using LDAP for user provisioning, you know that only active users in your corporate directory will be able to do any SCM operations at all. By using LDAP for authentication, you know that your corporate password standards will be enforced.

When using LDAP provisioning, all information about groups is based on LDAP. By combining this with AccuRev Access Control Lists, you can be assured that when a new user is given access to AccuRev, they will automatically be authorized for exactly the access that they need.

Extensible Controls

With fully configurable Workflow, Streams, and Access Control, AccuRev provides a wealth of compliance capabilities. If you need something beyond what is provided, you can use AccuRev's APIs and triggers to customize AccuRev to your exact needs.

AccuRev provides command line, XML, Java, and Perl APIs . Triggers are available for client and server pre and post operations which can call out to programs or scripts written in any programming or scripting language.

Support for Audits

Auditors want to validate that you follow a documented and compliant process. The easier it is for them to understand your process the easier it will be for them to validate that it is compliant and that you follow it. That translates into a faster audit.

AccuRev's side-by-side StreamBrowser and Workflow diagram enable a visual self-documenting process (see figure 3) which is instantly understandable without the need to create and update external documentation.

Not only do these tools make your process clear to auditors, they make it clear to everyone on the team exactly what the process is on a daily basis.

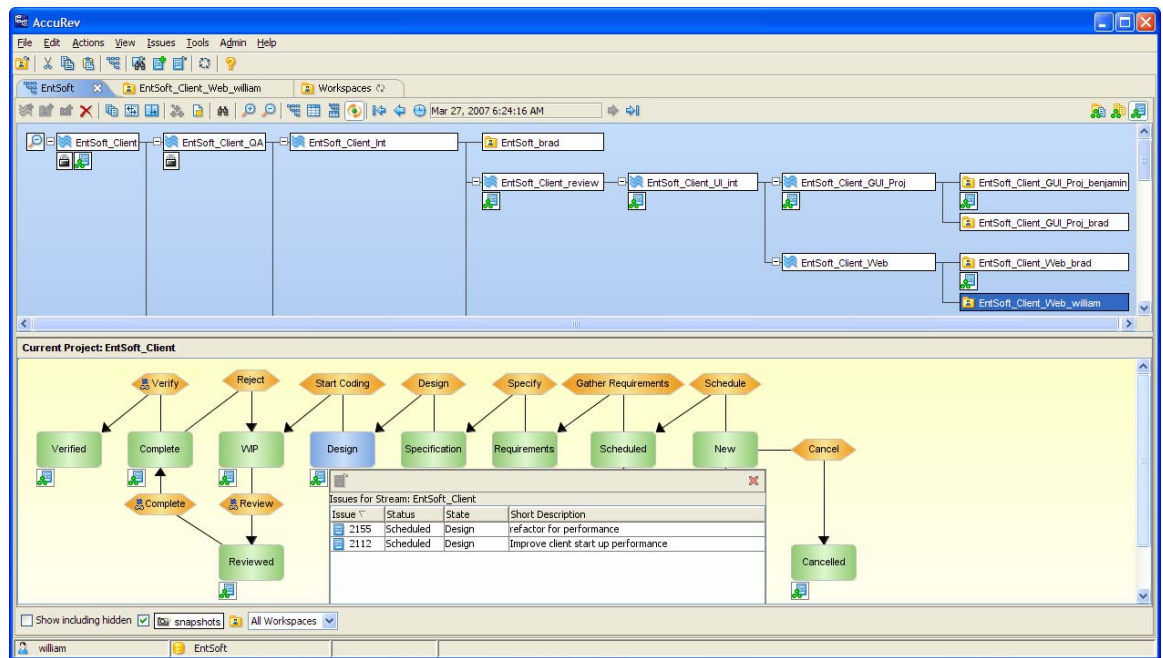


Figure 3: visual self-documenting process

In addition, AccuRev provides facilities for reporting on who did what, when, where, and why. Each operation in AccuRev creates an entry in the transaction log which records who performed the action, exactly what was done, when the action was performed, which files were affected, and the reason for the action. This information can be reported on in many ways. For instance, you can get a list of all files changed for a given project during a given timeframe, a list of all actions performed by a particular user, a list of all actions performed by all users on all projects, etc (see figure 4).

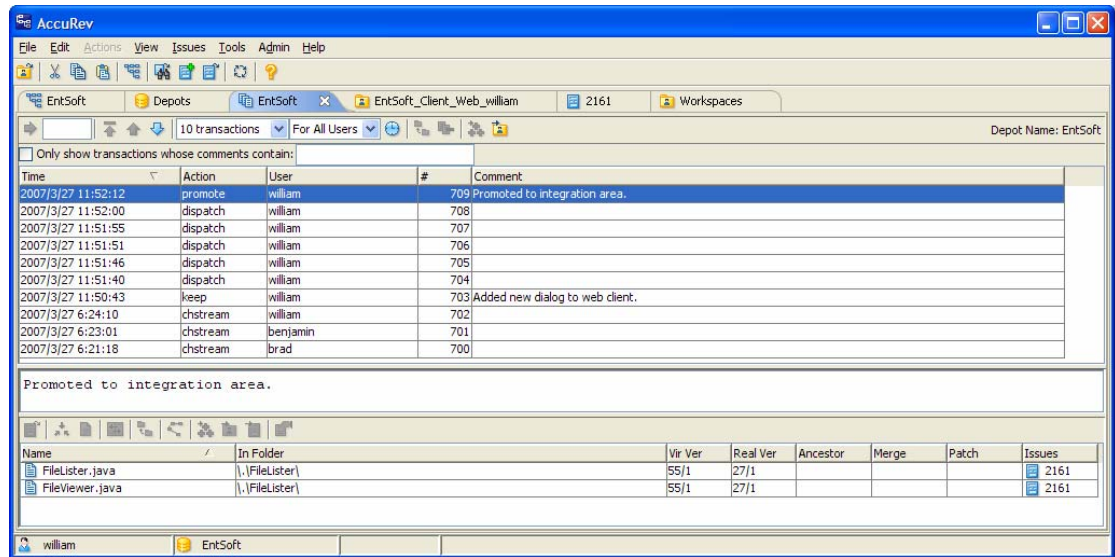


Figure 4: reporting on who did what, when, where, and why

Keeping Up with Change

There are many reasons why your current process may need to change. You may be just starting to implement a compliant process, an audit may have turned up a problem, there could be an update or change to the rules that govern your industry, or you may be entering new markets with different compliance issues. Whatever the reason, the more flexible and automated your process is the faster you can make the transition and the less it will cost you to implement it.

AccuRev is designed around the philosophy that change is inevitable. In support of this philosophy, everything in AccuRev is configurable and flexible with good defaults to start from. For example, unlike file-based SCM systems that operate on a file-by-file basis, AccuRev allows you to reconfigure your process model with fast and easy drag-and-drop operations that remove the need for scripting and guesswork.

Conclusion

SCM is an important part of any compliance initiative. AccuRev helps with the implementation, enforcement, documentation, and auditing of compliance. To top it all off, instead of reducing productivity as part of providing compliance, AccuRev will actually significantly enhance productivity.