Addressing Compliance Requirements
with IBM Rational ClearCase and IBM Rational ClearQuest
September 2005

Rational® software

Compliance-Driven Development

How IBM Rational change management solutions can help companies address compliance requirements

Karen Wade, Product Marketing Manager

Contents

Introduction

For companies in both the public and private sector, meeting regulatory compliance is not an option. Companies that can't or won't meet these new standards can face hefty fines and sanctions, class-action lawsuits, shattered public images, and even the possible imprisonment of company executives and board members.

These regulatory requirements and industry mandates are significantly affecting how companies develop and modify the applications they use to run their businesses. Companies need to deploy software development infrastructures that deliver the security, traceability, and repeatability features that can help them ensure that their software development architectures and processes are audit-ready.

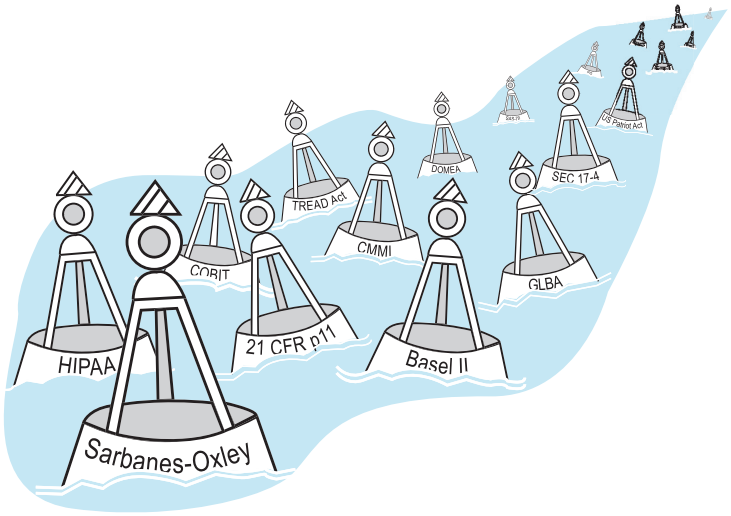
This paper discusses the compliance landscape and some key issues that companies face today. It examines the link between compliance and application development, and outlines the requirements for compliance-driven development. And finally, it discusses how IBM Rational change management products can provide a foundation for flexible compliance-driven development that can help companies meet a host of complex and evolving regulations and mandates.

Understanding the compliance landscape

Today's regulatory landscape consists of a mixture of cross-industry, industry-specific, and company-specific rules and mandates—each with its own unique standards and guidelines.

Most large organizations need to comply with at least one set of government-mandated or agency-mandated regulations, and many organizations must comply with multiple sets of regulations. These regulations and standards are extremely diverse, and oftentimes do not provide clear guidance on the steps that companies must take to comply. In fact, different audit firms can provide different guidance on the same mandates.

Sea of Regulations and Standards



In addition, new regulations are continually being introduced, and existing regulations change on a frequent basis. Businesses must keep up with current and emerging laws, regulations, and standards. This means companies not only need to get into compliance, but they need to stay in compliance.

The link between compliance and application development

Often, compliance projects imply IT projects. One reason is that making business applications compliant requires revisions to running applications. While different regulations place different requirements on development teams, they often tend to mandate that companies put proper controls and safeguards in place to ensure that changes made to business applications are made only by authorized individuals, and that those changes are auditable, traceable, and verifiable. For example, companies must design, code, and test applications that support financial transactions or financial reporting with auditability in mind. IT is so pervasive at most companies that any examination of internal controls is bound to turn into a de facto audit of IT.

Many organizations have resorted to manual systems for process management, record-keeping, and audit trails. These manual systems create overhead that place additional requirements and workload on development teams, making it harder for the IT organization as a whole to focus on the applications that deliver real business value.

Developing a compliance-driven framework

To address compliance challenges without the manual overhead, companies can implement a software development architecture that provides capabilities specific to compliance management, including:

- ***Workflow management:*** *Ensure consistent, repeatable processes across the application lifecycle, including notification and signoff processes, with electronic signatures.*
- ***Auditability/traceability:*** *Trace the origin and detail of all activities that take place during the software development process, who participated in those activities, when, and why. Verify and document authorizations and sign-offs for software changes.*
- ***Access control:*** *Provide user authentication to ensure that only authorized people make changes, and that roles are clearly defined with appropriate "separation of duties". Provide a robust centralized repository so that all development assets from requirements through test are captured and versioned in secure way.*

Software change management tools that automate and enforce development processes, provide audit trails and electronic records of changes, and provide access control are key to improving productivity and help toward achieving ongoing, sustainable compliance.

Change management: The foundation for an audit-ready infrastructure

IBM Rational change management tools streamline and automate change across the application lifecycle. IBM Rational ClearCase provides management and control of software development assets. IBM Rational ClearQuest automates workflow management. These products can improve automation of the software lifecycle, improve team productivity, improve visibility into project status and health, and improve control over the development process. They can also provide a foundation for an audit-ready infrastructure that can help reduce the cost of compliance.

Enterprise-wide workflow management

IBM Rational ClearQuest provides automated, customizable workflow management for consistent, repeatable processes. With Rational ClearQuest, users can define and enforce policies around change management. Alerts and notifications can inform team members of changes or updates. Approval and notification workflows can be established for closure.

Audit trails and traceability

IBM change management products provide full auditability and traceability of changes—whether to source code or other software assets, including requirements, design documents, models, test plans, test results, or any other project-related information.

Rational ClearQuest provides a comprehensive audit trail capability. Development teams can specify the exact records that should automatically get an audit trail when created or updated. When data is changed, Rational ClearQuest tracks who changed what, when, and why.

Electronic signatures are essential in establishing authorization or approvals. Rational ClearQuest provides electronic signatures to allow organizations to document authorizations and signoffs at key stages in the application lifecycle.

Rational ClearCase automatically records operations against objects stored in its repository. Additional features, like history tabs, show the various activities undertaken during the development process, and automated history reports are available on folders and files.

Rational change management products also provide a build audit capability, which enables organizations to create a record of the files that were used to create an application and which versions of code have been deployed to production.

Document/file version management

Rational ClearCase offers software development teams a secure, versioned repository in which to store digital assets created throughout the development lifecycle, from requirements through test. The check-out/edit/check-in process creates an automated audit trail of changes that were made to assets, when those changes took place, and who made them.

Access control

Rational change management products provide access control via industry-standard authentication services, such as LDAP servers and Microsoft® Active Directory. For authorization control, Rational ClearCase leverages the operating system on which it is installed. This means you can leverage the users and groups that have already been established in your operating system to set the authorization rules for Rational ClearCase. Rational ClearQuest includes its own user database for authorization control. It also lets you customize access control for key security checkpoints through scripting. These features help to ensure that changes are made only by authorized people.

In addition, Rational ClearCase allows you to control access down to the file level, establishing exactly which development team members can access particular files and what actions they can take on those files. Teams can use electronic signatures in Rational ClearQuest to confirm authorizations for specific actions.

Real-time reporting

Rational ClearQuest enables companies to generate reports of activities and changes that were made during the development process virtually any time, anywhere. Rational ClearQuest delivers comprehensive support for queries and offers a host of flexible and customizable charting and reporting capabilities that personnel with specific access rights can access. This enables better insight and visibility into projects for improved decision-making.

Protection of software assets and records

The loss of software assets and change records due to disruptive events, such as system and network failures or natural disasters, can have dire consequences for companies being forced to maintain comprehensive audit trails. IBM Rational change management products help alleviate these concerns by providing automatic replication and synchronization of assets and configurations to help companies maintain business continuity in the event of disaster.

The foundation of a complete, integrated compliance solution

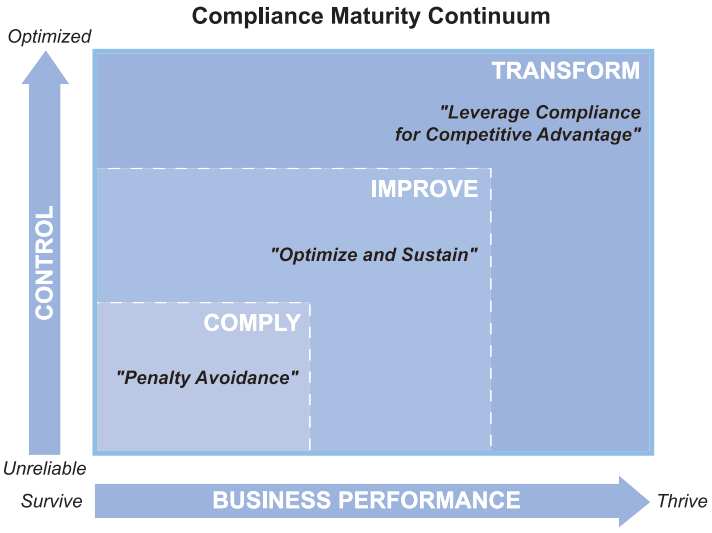
IBM Rational ClearCase and IBM Rational ClearQuest work seamlessly together for a complete and automated change management solution. They provide the flexibility, scalability, security, and reliability required for an enterprise-class solution.

Integration with IBM Rational Team Unifying Platform and IBM Rational Suite can provide lifecycle support across development disciplines. You can manage assets from requirements through test and alert team members to the affect of change.

Rational ClearCase and Rational ClearQuest are core components in the IBM Rational Software Development Platform, a complete, proven, open, and modular solution for application lifecycle management. By integrating with application lifecycle management tools, Rational ClearCase and Rational ClearQuest provide a foundation for a broader lifecycle solution, and can make compliance easier by providing workflow management and audit trails of changes across the software lifecycle.

Conclusion

The constantly changing regulatory landscape is forcing companies to rethink their current methodologies for addressing compliance. Long gone are the ideas that individual, one-time projects that focus on specific departments and business processes can address compliance requirements. Instead, compliance initiatives must consist of stable, flexible, and sustainable processes that cut across the entire enterprise—and help companies move from viewing compliance as simple penalty avoidance to leveraging it as a competitive advantage.



IBM Rational ClearCase and IBM Rational ClearQuest change management solutions deliver the foundation for software development environments that are audit-ready and tamper-resistant. They can help ensure that all changes to business applications are managed securely, in accordance with established policy, by the individuals who are authorized to make those changes. The bottom line is increased flexibility, improved control, and reduced cost of compliance.

For more information

To learn how IBM Rational ClearCase and IBM Rational ClearQuest can improve productivity and help you meet the complex and evolving challenges of compliance, visit: **ibm.com/software/rational/offerings/scm.html**

To learn more about how to manage for compliance with the IBM Rational Software Development Platform, visit: **ibm.com/software/info/developer/solutions/compliance/index.jsp**

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
All Rights Reserved
09-05

G507-0968-00