Manage Risk and Compliance with IBM Rational Compliance-Driven Development Solutions

Highlights

- ***Help reduce the cost of complying with Sarbanes-Oxley, Basel II, HIPAA, FISMA, 21 CFR Part 11, and other regulatory requirements.***
- ***Establish a sustainable, compliance-driven development infrastructure that is resilient to change.***
- ***Help automate the enforcement of any process framework, including COBiT, CMMI, Six Sigma, or your own enterprise risk management framework.***
- ***Provision regulatory policies, and understand their impact on the IT environment.***
- ***Help ensure that regulatory policies are properly defined, implemented, and validated.***
- ***Support the establishment of an audit-ready software development environment.***
- ***Establish the foundation for effective IT governance and business transformation.***

Regulatory compliance: A requirement and an opportunity

For both public and private sector organizations, meeting regulatory compliance requirements is an operational mandate. If you operate within a heavily regulated industry —such as financial services, health sciences, government or defense —your organization is likely governed by hundreds of regulatory mandates enforced by thousands of internal business and IT controls. Since 2002, every public company with more than $75 million in revenues has been subject to the provisions of the Sarbanes-Oxley Act.

Regulatory compliance measures are a necessary cost of doing business, and they can be expensive to implement. However, they don't have to tax your team's software development productivity. By adopting a strategic framework for regulatory compliance management, you can simultaneously improve software development productivity *and* reduce the risk of non-compliance with industry regulations.

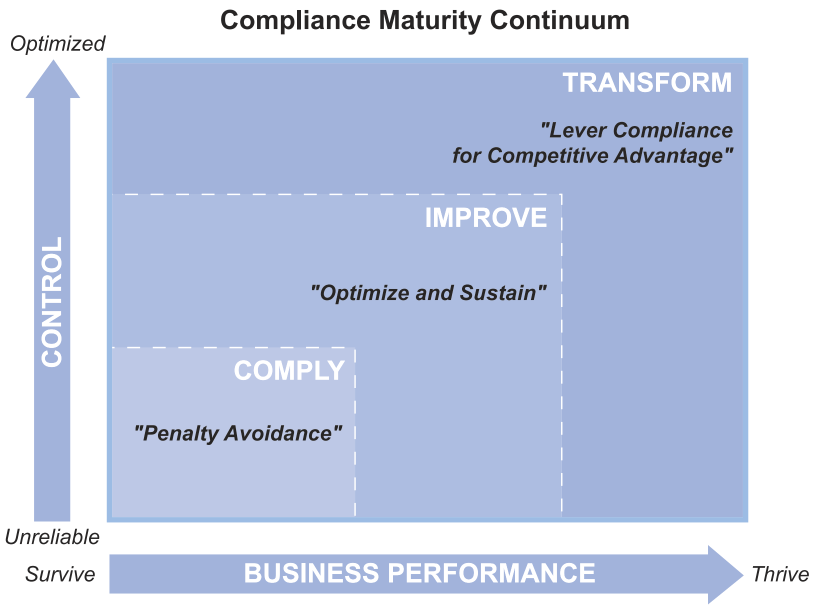

Figure 1. The Compliance Maturity Continuum illustrates the relationship between IT controls maturity and business transformation. Organizations with greater control over their IT processes can leverage this maturity to achieve sustainable competitive advantage.

IBM Rational provides proven solutions to mitigate the regulatory risks associated with the development, validation, and deployment of software assets—including those that automate your company's financial processes. The foundation of this approach is a scalable software development platform that can help your team:

- *Reduce the cost and manual effort required to comply with Sarbanes-Oxley, Basel II, HIPAA, 21 CFR Part 11, FISMA, and other regulatory requirements on a sustainable basis.*
- *Adopt process frameworks, including COBIT, CMMI, Six Sigma, or your own process framework, to provide actionable guidance and yardsticks for continuous process improvement.*
- *Establish a compliance foundation that is resilient to change as organizations, regulations, and IT priorities evolve.*
- *Adopt a business-driven development approach that better aligns technology investments with business objectives.*

> *"IT is so pervasive at most companies that any examination of internal controls is bound to turn into a de facto audit of IT."*[1]
>
> Steve Hill
> Managing Partner, KPMG

Compliance and software development

In an IT organization, compliance should begin with the software applications you develop and implement. Today's applications —comprising packaged applications, legacy systems, and new development projects—help automate virtually every aspect of your business. As a result, your organization's business processes are only as secure, auditable, and transparent as the applications that create and maintain them. As Managing Partner Steve Hill of KPMG explains, "IT is so pervasive at most companies that any examination of internal controls is bound to run into a de facto audit of IT."[1]

An investment in compliance-driven development tools and processes can help your organization avoid the cost, chaos, and disruption that can ensue from an audit failure. A comprehensive approach will help your organization:

- *Provision regulatory policies, and understand their impact on the IT environment.*
- *Ensure that regulatory policies are defined, implemented, and validated in key applications.*
- *Establish an audit-ready and tamper-resistant software development environment for controlling changes and documenting adherence to internal control structures.*
- *Manage regulatory compliance projects by actively prioritizing, monitoring, and measuring planned activities against results.*

Frameworks for regulatory compliance

Standards-based frameworks can help IT organizations align their methods and procedures with generally accepted IT management best practices. The most popular frameworks include:

- *The COBIT (Control Objectives for Information and related Technology) framework, governed by the Information Systems Audit and Control Association (ISACA)*
- *The CMMI (Capability Maturity Model Integration®) framework, governed by the Carnegie Mellon Software Engineering Institute (SEI)*
- *The ITIL (IT Infrastructure Library) framework, governed by the United Kingdom's Office of Government and Commerce (OGC)*

Whether you adopt all of the guidelines within one of these frameworks or tailor them for your own needs, IBM Rational's compliance solution can provide valuable support. The Rational solution:

- *Automates the fundamental principles of software development oversight, including process enforcement and guidance, lifecycle requirements traceability, continuous validation, metrics analysis, and project management and measurement.*
- *Can be customized to your exact process, workflow, and reporting requirements.*
- *Has been proven in thousands of successful engagements, supporting a broad spectrum of process and standards frameworks.*

[1] *CFO Magazine, "Sarbox Surprises", June 22, 2005*

- *Automates implementation of the IBM® Rational® Unified Process®, or RUP®, a flexible, iterative software development process framework that can deliver customized process guidance to your team.*

RUP has been successfully used to support adoption of COBIT, CMMI, ITIL, and other frameworks that support enterprise risk management. Its configurable architecture enables you to tailor the process components you need for each stage of your software development project. Incorporating best practices adopted by hundreds of organizations and taught in hundreds of universities, RUP methodology is the *de facto* industry-standard software development process.

A more Rational approach to regulatory compliance

The IBM Rational compliance solution provides the foundation for effective IT oversight and improved team productivity. This solution supports all three dimensions of compliance-driven development:

- ***What you build:*** *Demonstration that all compliance mandates are accurately captured and implemented in key applications.*
- ***How you build it:*** *Demonstration that all software changes are made in a secure, audit-ready environment, subject to appropriate IT controls at key lifecycle checkpoints.*
- ***How you manage it:*** *Demonstration of effective fiscal management and oversight of your IT portfolio and compliance remediation projects.*

This three-dimensional approach supports a comprehensive, compliance-driven development program via the following capabilities:

- *Lifecycle requirements traceability* to help auditors verify that compliance requirements were accurately captured and implemented in key applications.
- *Auditable workflow management* capabilities that help ensure software changes were made by authorized personnel for valid business reasons.
- *Flexible metrics and reporting, electronic signature, and audit trail* capabilities that can be tailored to the exact processes and IT controls that govern your development environment.
- *Verifiable software builds* to help ensure and document that you are deploying the correct software.
- *Continuous validation* of compliance mandates through integrated test management.
- *Metrics management* that demonstrates adherence to a well-defined compliance process.

The Rational compliance-driven development solution is delivered through IBM Rational Portfolio Manager, IBM Rational RequisitePro®, IBM Rational ClearCase®, IBM Rational ClearQuest® and IBM Manual Tester, and can be extended by complementary offerings within the IBM Software Development Platform.

> *"Any application that supports a financial transaction or financial reporting must be designed, coded, and tested with auditability in mind."*[2]
>
> Margot Visitacion
> Vice President
> Forrester Research

What you build: Managing compliance requirements

Risk officers, business analysts, and compliance officers face multiple challenges in implementing compliance mandates across the enterprise. They must:

- *Provision IT policies in an environment of continuously evolving legislation and regulatory re-interpretation.*
- *Manage the implementation of compliance mandates across dozens or hundreds of IT applications.*
- *Continuously validate that IT applications meet compliance requirements over time, as both systems and policies evolve.*

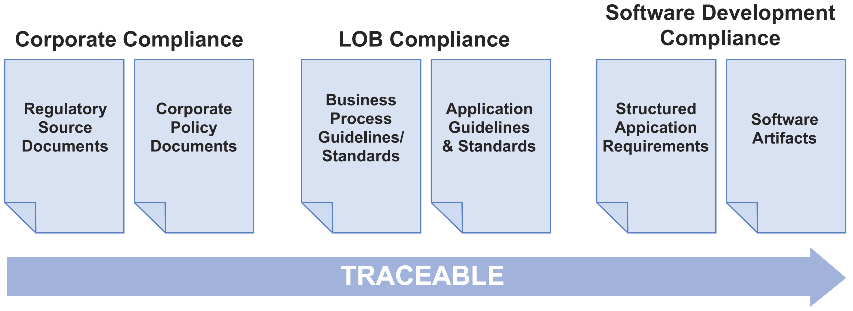
Corporate Compliance
LOB Compliance
Software Development Compliance
Regulatory Source Documents
Corporate Policy Documents
Business Process Guidelines/ Standards
Application Guidelines & Standards
Structured Appication Requirements
Software Artifacts
TRACEABLE

Figure 2. Policy management involves stakeholders across the enterprise. IBM Rational RequisitePro can help your organization trace the impact of policy decisions across Corporate, Line-of-Business, and IT organizations.

[2] *"Sarbanes-Oxley Will Drive Project Management Maturity—But Maybe Not Quickly Enough", Margot Visitacion, Forrester Research, May 2, 2003*

The IBM Rational RequisitePro solution is a requirements and use case management tool that can help teams:

- *Provision policies across the enterprise* by providing traceability from legislation to policies to compliance requirements in a seamless, bidirectional way.
- *Trace compliance requirements through the software development lifecycle*, by linking compliance requirements to use cases, test artifacts, defect and change management artifacts, and software build documentation.
- *Continuously validate compliance requirements* through integrations with test management solutions.

In combination, these capabilities enable organizations to ensure that compliance mandates are accurately captured and implemented across enterprise applications.

Provision policies across the enterprise

Changes in regulatory policy can have sweeping effects on how your enterprise does business. New legislation—or a reinterpretation of existing legislation—can result in downstream changes to dozens of policy documents and hundreds of supporting business controls. A risk officer or analyst may be charged with capturing, interpreting, communicating and managing these policies over time. This means they must know:

- *Who is responsible for regulatory interpretation?*
- *Who has signed off on policies affected by regulations?*
- *Which IT systems are impacted by specific policies?*
- *What documents prove that the policies are captured and implemented in these IT systems?*
- *As systems or policies change, what are the compliance risks?*

IBM Rational RequisitePro enables organizations to maintain a policy repository that maintains a “chain of traceability” among policy -related artifacts. It helps risk officers, business analysts, and compliance managers:

- *Capture regulations in familiar Microsoft Word documents.*
- *Tag and store regulatory text as “policy artifacts” that can be managed through structured data techniques.*
- *Document discussions and key decision points that contributed to policy interpretation, to provide a record of evolving policy decisions over time.*
- *Provide a centralized storage location for all regulatory policies affecting the business, with centralized linkage to multiple project artifacts.*
- *As legislation and its interpretation evolves, easily identify which policy decisions and systems may be impacted by changes.*
- *As systems are redesigned or updated, easily identify the relevant policy decisions that must be satisfied.*

These capabilities bring new rigor and structured management techniques to one of the most complex tasks facing risk officers, business analysts, and compliance managers.

Enforce mandates through software automation

Once you establish compliance policies, you will want to automate or implement a subset of these policies through changes to software applications. IBM Rational RequisitePro can help you track the definition, design, and implementation of these policies, from requirements elicitation through deployment. Through integration with other software development tools, IBM Rational RequisitePro provides:

- *Direct access to the compliance policies from developers’ Integrated Development Environments (IDE). This helps ensure that developers will implement them as specified.*
- *Linkage between compliance policies and design documents created with IBM Rational modeling tools. Developers can easily review and assess the impact of these policies on design elements and stay informed about changes that may impact their work.*
- *Linkage between compliance policies and test results. As compliance mandates evolve, testers can run reports that highlight which test cases are impacted by the change. This helps ensure they will update those test cases to reflect the latest requirements.*

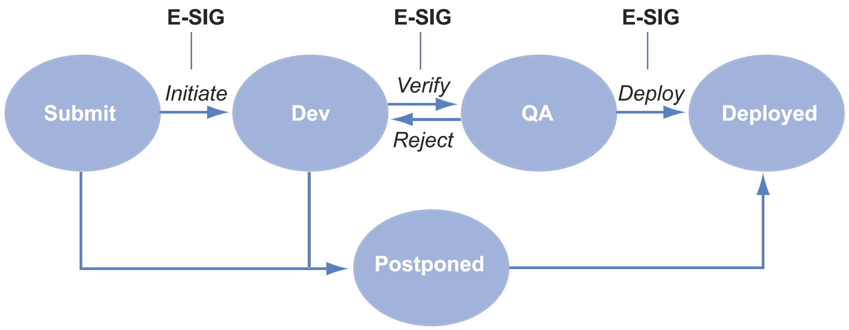

Figure 3. Internal control structures both automate and enforce software development oversight. This sample workflow with control checkpoints illustrates how a typical organization might automate their control structure using Rational change management solutions.

How you build it: Managing software changes and approvals in an audit-ready environment

Providing your development team with an organized, tamper-resistant and self-documenting software development environment is more than just good sense. For many organizations, it is a key requirement for complying with regulatory requirements, such as Sarbanes-Oxley, that may require documentation of sound internal control structures.

For software development teams, such a structure encompasses a standard process for managing IT approvals at relevant stages in the software development lifecycle. A typical IT control structure may require that:

- *All software change requests be approved by a Change Control Board.*
- *All releases to production be validated by a Quality Assurance Board.*
- *All deployment rollout activities be approved by a Change Control Board.*
- *All changes to deployed software be made by authorized personnel for valid business reasons.*

The exact composition and details of a control structure may not be as important as the existence of an established process with agreed-upon workflow, defined documentation, and established signatory authorities.

Enforce controls with Rational change management solutions

Many organizations use manual systems to enforce internal control structures for change management, placing a burden on development teams that ultimately impedes the IT organization's ability to deliver business value. The IBM Rational automated change management solution, featuring IBM Rational® ClearCase® for software asset management and IBM Rational® ClearQuest® for defect and workflow management, provides a highly practical and customizable solution for teams who need to define, manage, enforce, and audit IT control structures for software development.

IBM Rational ClearCase provides lifecycle management and control of software development assets. As code and other software assets change over time, Rational ClearCase keeps a clear, detailed record of changes. It also helps secure code and other important documents from unauthorized access or damage.

IBM Rational ClearCase provides:

- *Version control* that records all changes to software assets over time.
- *Audit trails* that document the "who, when, and what" of every software change.
- *User authentication* to protect against unauthorized access to strategic software assets.
- *Baselines* to ensure that only the right versions of files are included in your releases.
- *Reporting* of real-time information on the status of activities and incorporation of change requests.
- *Build auditing* that guarantees the reproducibility of software versions. Rational ClearCase automatically detects dependencies and produces a detailed bill of materials that reports the exact file versions comprising a build.
- *Project policies and triggers* for flexible enforcement of site-specific configuration management policies.

IBM Rational ClearQuest is a powerful and flexible change tracking and workflow management system that provides the capabilities you need to establish, enforce, and document software development controls with a minimum of manual overhead. You can configure Rational ClearQuest to enforce custom processes and workflows. For example, you can specify which steps in your process require electronic signature authorization, what information is captured in the electronic signature audit trail, and which users have access to specific activities. Automating your team's control structure helps ensure that naïve or unethical users cannot circumvent it.

IBM Rational ClearQuest provides:

- *Workflow management* to define and enforce consistent, repeatable processes with flexible process definition and customization.
- *Audit trails* that capture and document evidence of who made a change, what they changed, and when they did it.
- *Electronic signatures* that help ensure that only authorized users can approve change requests and moves to production.
- *User authentication* with IDs and passwords that provide identify management protection.
- *Data controls* to ensure that only authorized users make changes to controlled data.

The power of Unified Change Management

In combination, IBM Rational ClearCase and IBM Rational ClearQuest support activity-based development by linking a named activity (such as "Bug Fix 302" or "Finance Release 102") with the set of assets supporting that activity. Activity-based change management provides auditors, managers, and team members with instant access to the "who, what, when, and why" of any software change. It allows teams to respond to auditors' requests to questions such as:

- *Who made changes to these financial documents and process documents?*
- *Where are the change request records authorizing those changes?*
- *When were the changes made?*
- *Why were the changes made?*

With this information at their fingertips, IT managers can improve the transparency of IT operations and streamline communication with business managers, auditors, risk analysts and compliance managers.

Protecting software assets and records

Disruptive events such as system and network failures or natural disasters can have dire consequences for companies who maintain comprehensive audit trail records. IBM Rational change management products help alleviate these concerns by providing automatic backup and restore capabilities that help companies maintain business continuity in the event of disaster. These products also provide automatic replication and synchronization of assets and configurations, to ensure that assets and records are available when needed.

How you manage it: Effective fiscal management and compliance project oversight through portfolio management

IT executives are charged with managing investments—and balancing risk and costs—across the entire portfolio of an organization's IT assets. In recent years, this responsibility has expanded to include executive oversight of the multi-year effort required to implement regulatory changes across the organization, controlling costs, budget, and delivery. IBM Rational® Portfolio Manager® is a solution that helps IT executives and project managers effectively track, manage, and prioritize their regulatory compliance projects, improve executive oversight, and reduce overall operational risk.

IBM Rational Portfolio Manager helps teams:

- *Track compliance remediation initiatives and progress.*
- *Demonstrate compliance through metrics and trend analysis.*
- *Mitigate regulatory risk through portfolio management activities.*

Track compliance initiatives and remediation progress

A persistent challenge in compliance management is gaining reliable insight into the status and delivery of multiple compliance remediation projects. IBM Rational Portfolio Manager provides technical and business stakeholders with the ability to visualize the complete IT environment, including complex project and portfolio metrics. Management dashboards communicate project status through tables, maps, and graphical displays, providing rollup project status of multiple compliance projects at-a-glance.

Demonstrate compliance through metrics management

Metrics analysis is one of the most valuable tools in the compliance management arsenal. Metrics are the means organizations use to demonstrate to auditors that they are following a well-defined compliance process. By demonstrating that forty change requests have entered the validation stage, for example, you can show that development team members are not circumventing the validation process. Trend analysis allows auditors to validate that the organization is adhering to stated process workflows. For example, if you can show that thirty of the forty change requests were deployed within three months, that implies that the validation and deployment processes are working. IBM Rational Portfolio Manager routinely collects and tracks such metrics, which supports the auditing process as well as objective business decision making.

Manage risks and issues

Risk and compliance are inextricably linked in modern enterprise risk management. However, most organizations do not have an easy way to quantify these risks and incorporate them in their software development prioritization and management activities. Rational Portfolio Manager centrally catalogues risks and responses. It describes and measures each identified risk event, based on its impact, probability, and precision rankings. By incorporating objective risk analysis data in their decision criteria, organizations can more effectively set priorities and make management decisions.

IBM: Your partner for regulatory compliance management

IBM Rational solutions are based on a modular, scalable platform that is extended by other IBM products and services to provide the industry's most comprehensive approach to regulatory risk and compliance. Additional IBM solutions for regulatory compliance management include:

- ***Internal controls management:*** *IBM Workplace™ for Business Controls & Reporting (WBCR)* delivers a complete environment to document, evaluate, and report the status of internal controls across multiple initiatives within an enterprise, including compliance initiatives for Sarbanes-Oxley.
- ***Security:*** *IBM Tivoli* solutions help organizations manage the security, access, identity, and configuration of business-critical systems.
- ***Archival and Retention:*** *IBM DB2* solutions can help organizations establish and enforce archival and retention solutions for regulatory compliance. The IBM Banking Data Warehouse product is specifically designed to help meet Basel II requirements.

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Printed in the United States of America
08-05

*Rational ClearQuest integrates with Crystal Reports Professional Edition for advanced reporting capabilities.

The Rational Software home page on the Internet can be found at **ibm.com/rational**.

The IBM home page on the Internet can be found at **ibm.com**.

♲ Printed in the United States on recycled paper containing 10% recovered post-consumer fiber.

G507-0963-00