White Paper
September 2009

Tivoli® software

Rational® software

Addressing IT governance, risk and compliance (GRC) to meet regulatory requirements and reduce operational risk in financial services organizations

Contents

Executive summary

Effective IT governance, risk and compliance (GRC) is essential for financial services organizations to meet increasingly stringent regulatory and audit requirements and reduce business operational risk. By instituting the appropriate IT GRC controls, organizations can demonstrate regulatory compliance in areas of specific concern to auditors. At the same time, these controls can take organizations beyond the immediate need to pass an audit and into the realm of reduced operational risk exposure through process improvements. IBM offers extensive capabilities through its IBM Tivoli® and IBM Rational® software offerings to help financial services organizations deal with specific regulatory and audit requirements, as well as with issues affecting long-term, ongoing risk management.

Negotiating a complex and dynamic regulatory and audit landscape

In practical terms, meeting every set of regulatory and audit requirements is a tremendous undertaking, given the number and scope of regulations that financial services organizations face, and the multitude of controls that must be put into place to comply with these regulations and to pass audits (see Figure 1). Not all organizations must conform to all of the regulations, however, or institute every possible control; it depends on a number of factors, including the jurisdiction in which a company operates and the type of business it conducts. For example, SB 1386 is a law that applies only to companies that have customers or employees in California. And HIPAA, or the

Health Insurance Portability and Accountability Act, is a U.S. healthcare industry-specific law whose requirements apply only to financial services companies that are engaged in business that touches on healthcare and health information.

Major IT control objectives for a regulation subset

	SOX	HIPAA	GLBA	SEC	Basel II	USA Patriot Act	SB 1386	PCI/CISP
Manage change	X	X	X	X	X		X	X
Ensure system security	X	X	X	X	X	X	X	X
Manage configuration	X	X		X	X			X
Manage problems and incidents	X	X		X	X			X
Manage data	X	X	X	X	X		X	X
Manage operations	X	X	X	X	X	X	X	X
Manage third-party services	X	X	X	X	X	X	X	X
Acquire or develop application software	X			X				
Acquire technology infrastructure	X			X				
Develop and maintain policies and procedures	X			X				
Install and test application SW and infrastructure	X				X			
Define and manage service levels	X	X	X	X	X	X	X	X
Validate customer data and protect privacy		X	X		X	X	X	X
Manage application controls	X	X	X		X	X	X	X

Meeting regulatory requirements is a challenge that requires financial services organizations to have multiple combinations of IT controls in place.

Highlights

Regulatory compliance presents a daunting challenge involving multiple sets of requirements and varying combinations of controls to enable and demonstrate compliance.

Simply passing an audit does not necessarily mean an organization is effectively managing operational risk—only that the organization is capable of passing the audit.

Although it's true that all regulations do not necessarily apply to all organizations, regulatory compliance still presents a daunting challenge involving multiple sets of requirements and varying combinations of controls to enable and demonstrate compliance. Furthermore, the already-crowded regulatory landscape is only going to grow more so. Another wave of regulation is emerging as the result of recent financial upheavals, and legislative bodies are already implementing new rules governing the financial services industry worldwide. Financial services organizations must be prepared to meet the additional regulatory and audit requirements that will arise.

Managing compliance in five key areas

To address concerns about complying with regulations and passing audits, financial services organizations should recognize that there are generally five key areas in which auditors will seek evidence that an organization has effective IT controls in place (see Figure 2). Organizations must demonstrate effective controls in all five categories to pass regulatory compliance and IT audits. And beyond the immediate need to pass an audit, having effective controls in place in these areas also provides a strong information foundation for operational risk management and reporting, to help address ongoing business risk. This is important because simply passing an audit does not necessarily mean an organization is effectively managing risk—only that the organization is capable of passing the audit. To pass audits and effectively manage operational risk requires a proactive GRC infrastructure.

Highlights

IT governance and risk compliance audit classification

Category	Examples
Access	Physical security Logical security
Segregation of duty	Identity access management Roles Access rights
Change management	Asset management Version control Provisioning
IT operations	Service management Incident management Batch support Backup/restore Network Infrastructure management
Application development	Software development lifecycle support User acceptance testing Unit testing

Financial services organizations must demonstrate effective controls in five major categories in order to pass regulatory compliance and IT audits.

The remainder of this paper describes each of the five categories in detail and presents examples of financial services organizations that have successfully addressed them using IBM solutions.

Access

Access to sensitive information must be protected both on a physical (systems) level and on a logical (data) level.

Controlling access to information appropriately is an important component of compliance because so many regulations address the privacy and security of sensitive data. For example, in the U.S., the Gramm-Leach-Bliley Act includes provisions to protect consumers' personal financial information held by financial institutions. Controlling access is challenging not only because of the

Highlights

number of regulations, but also because of the number of different types of IT systems, networks, applications and data formats that may exist across an organization. Access to sensitive information must be protected both on a physical (systems) level and on a logical (data) level.

IBM offers a number of different capabilities to address data protection, focusing particularly on access management. These capabilities are designed to ensure that people who require legitimate access to information have it when they need it, and that people who should not have access do not, as well as to demonstrate appropriate access to auditors. IBM solutions help ensure that access policies are congruent at the business, architectural and IT operational levels. They are designed to enable centralized management of access policies, to minimize inconsistencies and errors that can result from attempting to manage them at multiple points.

A large South American bank is using IBM solutions to securely manage the entire customer access lifecycle, from account creation to termination.

To meet access management needs, a large retail banking operation in South America deployed a solution that brings together IBM Tivoli Access Manager, IBM Tivoli Directory Integrator, and IBM Tivoli Identity Manager. Using these products in combination with an IBM Service Management solution for security, the bank is able to securely manage the entire customer access lifecycle, from account creation to termination. The solution improves access control by automatically identifying and removing "orphan" accounts and by providing greater accountability and auditing associated with password usage. It also improves governance by simplifying compliance reporting. The result is an environment in which controls are in place not just to demonstrate that the bank is conforming to regulatory requirements for keeping information private, but also to ensure that the privacy of that information is maintained on an ongoing basis.

Highlights

Identity and access management solutions such as Tivoli Identity Manager enable IT administrators to avoid issues related to separation of duty by provisioning users and managing roles methodically and efficiently.

Segregation of duty

Segregation of duty is an aspect of access control that constitutes a key requirement of the Sarbanes-Oxley Act of 2002 and similar laws outside of the U.S. Segregation of duty refers to the need to make sure that no one person performs multiple duties or fills multiple roles in such a way as to constitute a conflict that could compromise the integrity of business data. For example, someone who is responsible for issuing purchase orders should not also be responsible for issuing checks. After a merger in the financial services industry, there may be confusion about user roles—if a teller is called an "associate teller" in one bank and an "assistant teller" in the other, for example—which could lead to a lack of clarity about which privileges are appropriate for an individual based on his or her role. This lack of clarity puts the organization at greater risk for failure to segregate duties appropriately. Identity and access management solutions such as Tivoli Identity Manager enable IT administrators to avoid issues related to separation of duty by provisioning users and managing roles methodically and efficiently.

An international bank based in Australia has integrated IBM Tivoli software into its IBM WebSphere® portal application infrastructure, using capabilities for identity and access management to improve access to bank resources. The organization addresses segregation of duty and other access concerns by providing employees with appropriate access to different applications based on their roles. The software also improves employee productivity by enabling users to gain access to those applications, when they need to, without having to enter different passwords or be reauthenticated.

IBM provides a process-automation engine for facilitating change management, helping to ensure that changes to the IT infrastructure are executed with minimal risk.

Change management

Operational risk is an inevitable consequence of change, but this risk can be reduced or managed in the IT environment with the right change management controls in place. Change management provides a methodical way of accommodating inevitable change in the IT infrastructure so that any associ-

Highlights

ated risk is minimized. IBM provides a process-automation engine for this purpose. When change is introduced, the IBM solution automatically ensures that the necessary tasks occur on time and as planned. This approach reduces the chance of errors or oversights in the change process that could create business operational and compliance risks by compromising operations or security.

IBM helped a Swiss financial services company streamline their change management processes, resulting in the consolidation of 40 distinct change processes into one.

A Swiss financial services company turned to IBM to help streamline their change management processes. IBM's solution for the company consolidated 40 change processes into one, using IBM Rational Method Composer, IBM Tivoli Change and Configuration Management Database (CCMDB), IBM Tivoli Release Process Manager, IBM Tivoli Provisioning Manager and IBM Tivoli Asset Management for IT software. These integrated Rational and Tivoli solutions enabled the firm to move away from a siloed, manual approach. As a result, the company has both reduced operational risk by improving its governance of service management and reduced compliance risk by enhancing its ability to address regulatory requirements.

Asserting appropriate controls over IT operations helps financial services organizations make sure that systems and networks are running properly and that data is protected against the risk of compromise due to operational failures.

IT operations

Asserting appropriate controls over IT operations helps financial services organizations make sure that systems and networks are running properly and that data is protected against the risk of compromise due to operational failures. By ensuring proper operations, the organization protects itself against both business operational risk and compliance risk. Historically, banks have used past loss data as the foundation for reducing the chances of operational failure. However, quantitative impact studies by banking regulators indicate that continuous, automated monitoring is more beneficial than the study of past data as a means of preventing future problems.1,2 IBM helps financial services organizations keep IT operations running smoothly by providing

Highlights

IBM helped one financial institution establish a Command Center to maximize service availability and performance, resulting in the prevention of roughly 500 service disruptions.

technology and services to comprehensively monitor IT events, report on event cause-and-effect, and track the business operations impact of IT events—and delivering critical information directly to the desktop through customizable dashboard views.

As part of one financial institution's initiative to maximize service availability and performance, IBM worked with the company to establish a Command Center from which to monitor services delivery and interdict service disruptions. The Command Center leverages IBM Tivoli application monitoring tools to reduce the risk of disruptions and remediate performance issues related to critical business processes. In its first year of operations, the Command Center prevented roughly 500 service disruptions. In addition, it enabled the institution to identify and deliver 26 availability and quality improvement recommendations.

Application development

As regulatory change continues, IT organizations must respond by assessing applications to determine whether they comply with evolving regulatory requirements—and then, most likely, modifying them to meet those requirements. Even if many of a financial services organization's applications are from third parties, it remains the responsibility of the organization to ensure compliance when those applications change or are replaced by new ones. IBM Rational AppScan software can be a valuable tool in testing applications to ensure their integrity before rolling them out in a real-world production environment.

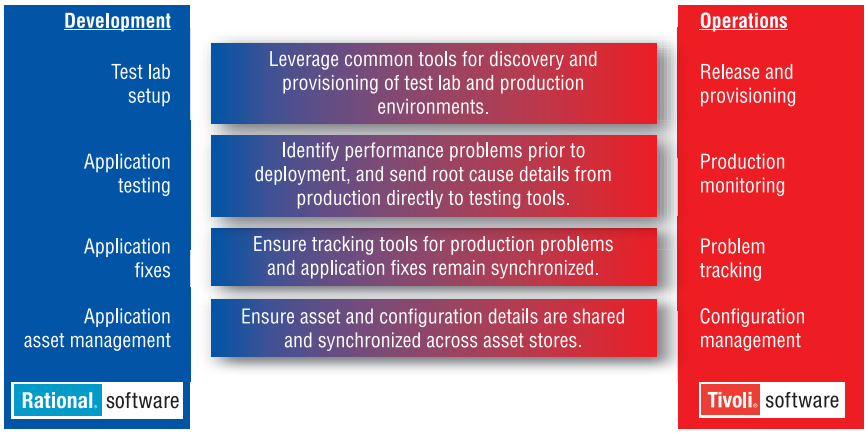
One asset servicing organization leveraged this software in its efforts to create new securities-transaction applications that incorporate more rigorous security practices. The company was able to use IBM Rational AppScan software to identity, analyze and remediate security issues from development through deployment.

Highlights

One of the most important concerns for IT is to smooth the path between application development and deployment, to ensure not only that the software is fully tested and fixed in development but also that it runs smoothly in production.

One of the most important concerns for IT is to smooth the path between application development and deployment, to ensure not only that the software is fully tested and fixed in development but also that it runs smoothly in production. Figure 3 shows how IBM Tivoli software and IBM Rational software work together to help bridge the gap between development and operations. Essentially, having both of these resources enables organizations to successfully perform application testing and fixes during development, using Rational AppScan software, and then to integrate those efforts into the production environment with IBM Tivoli change management software and other tools. The integrated environment enables the two areas to work together seamlessly and cost-efficiently.

Bridging the gap between development and operations



IBM Tivoli and IBM Rational software work together to bridge the gap between development and operations.

Realizing business benefits

The benefits of instituting IT controls to address the five major areas of concern to auditors extend beyond the ability to comply with regulatory requirements or to pass an audit. The IBM solutions described in this paper deliver IT GRC business benefits on several levels.

- **Reduce compliance and audit costs.** *IBM solutions help reduce the costs of regulatory compliance and audits by providing improved monitoring and oversight to management, and by improving regulatory compliance reporting. This can lead to better risk ratings.*
- **Reduce operational risk exposure.** *IBM solutions can help reduce operational risk exposure by providing key measures for "risk and controls matrices" assessments. They can improve business performance by identifying gaps and failing processes that need to be addressed.*
- **Reduce the cost of IT operations.** *IBM solutions can help reduce the overall cost of operations by providing an effective feedback loop between the development and operations components of IT, so that the two organizations can work together more efficiently and effectively to reduce operational risk exposure.*

For more information

To learn more about Tivoli and Rational solutions to help address IT GRC requirements in your financial services organization, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/Tivoli and **ibm.com**/Rational.

About Tivoli software from IBM

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation—visibility to see and understand the workings of their business; control to effectively manage their business, help minimize risk and protect their brand; and automation to help optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world—visit www.tivoli-ug.org

[1] Bies, Susan Schmidt, "Linkages between internal capital measures and regulatory capital requirements." Speech given at the International Center for Business Information's Risk Management Conference: Basel Summit, Geneva, Switzerland, December 6, 2005. www.federalreserve.gov/boarddocs/speeches/2005/20051206/default.htm

[2] Qualitative Impact Studies, Basel Committee on Banking Supervision. www.bis.org/bcbs/qis/index.htm

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

Produced in the United States of America
September 2009

Recyclable, please recycle

TIW14039-USEN-00