

A vertical decorative bar on the left side of the page, featuring a grey-to-white gradient and a pattern of thin, light grey lines forming a grid of overlapping triangles.

● Managing Regulatory Risk
Through Improved IT Processes

With increased pressure to adhere to auditory and regulatory requirements, Application Life Cycle Management plays a significant role.

Managing Regulatory Risk

IT executives are faced with the daunting task of managing risk for their enterprises by demonstrating regulatory, legal and fiscal compliance. With increased pressure from mandated regulations and with internal IT auditing functions becoming more involved in the IT organization, IT executives have to develop sound strategies to ensure that software development processes are defined and repeatable.

There are inherent business risks in not establishing these processes and procedures. Regulatory deadlines, non-compliance penalties, and jail time for executives who have personal responsibility for compliance are just some of the risks at hand. In order to minimize risk to the enterprise and to enable good corporate governance, IT executives and auditors are finding that application life cycle change management, with its emphasis on process management, plays a key role.

IT Audit Assessments for Regulation Compliance

Who is responsible for ensuring regulatory compliance? Typically it is the CIO's responsibility to determine where the risks are related to internal control within the IT organization. These risks are based on how the IT processes impact applications and data integrity. Typically it is the application and data owner, or business owner's responsibility, to work with the CIO in establishing effective controls to mitigate risks. IT organizations will be required to implement the automated aspects of internal controls. What are the important controls that help mitigate risks, and where do auditors look for failure?

Controls That Help Mitigate Corporate Risks

Change Management Processes

Change management provides assurances that applications function as intended and the integrity of processing is intact. Through these processes, access to applications and data are restricted so that inadvertent or deliberate changes to production data or other related components such as interface routines, background processing and updates do not occur. Together with security administration, application life cycle change management processes assures transactions can only be initiated, modified or deleted by appropriate individuals.

The impact of strong change management is that applications perform as designed, programmed controls function as designed, and access to transactions and data function as designed.

Segregation of Duties

The development of roles and transactions which need to be segregated are looked at. For example, the person responsible for changing code is separated by role from the person responsible for placing the changed code into production.

Access to Critical Transactions and Data

There needs to be a process to periodically review access to critical transactions and data, and to determine that authorized individuals have a valid business purpose in accessing this information. This review needs to have an audit trail.

Management of Technical Infrastructure

Problem management procedures related to errors in processing need to be in place. How problems are monitored and resolved also needs to be documented.

Auditors look at the above processes and activities only in the context of how the controls relate the ability of the company to meet their objectives for reliable financial reporting. Table 1 displays process components that are typically reviewed from an auditor's point of view. How can IT organizations assist auditors in helping review these controls and gain compliance? The implementation of automated change management and problem management holds the answer.

Control Items	Control Questions	Control Risks
Initiation of change requests	Are they properly initiated? Have they been approved by users? Are they being monitored?	Untested or unauthorized changes may be moved to production; changes may not address user needs.
Testing and approval of changes prior to migration into the production environment	Are the changes tested and approved? Have they been approved by the application and data owners?	Unauthorized changes may be moved to production.
Critical calculations, data validations, exception routines, interfaces	Have they been adequately tested from a functionality perspective?	Untested changes may be moved to production.
Job sequencing and relationships	Are they appropriate?	Erroneous jobs may be executed in inappropriate order.
Application migration procedures	What is the integrity of the process and the access to applications and data during the process?	Lack of procedures may result in untested and/or unauthorized changes.
Backout processes	Are they in place?	Increased chance of business process disruption and/or errors.
Validation of successful promotions to the production environment	Can promotions be validated?	Invalid changes may be moved to production.
Emergency change procedures and processes	Are they reviewed after the fact for validity and appropriateness?	Increased chance of business process disruption and/or errors.
Documentation and training updated	Has the system and user documentation been updated to reflect the changes to the application? Have users been trained on the system?	Users unaware of system changes which may increase chance of business process disruption and/or errors.

Table 1: The process components typically reviewed from an audit perspective

Supporting Regulatory Compliance with Serena Solutions

Serena Software offers robust, automated, process-oriented Application Life Cycle Management solutions, minimizing the risk of change-related failures by automating change throughout the enterprise. Working together, Serena® TeamTrack® and Serena® ChangeMan® product families automate and enforce orderly, efficient processes for managing fast, reliable changes to applications—regardless of platform.

As the Robert Frances Group states, “According to clients interviewed, the single most important factor in selecting and using Serena ChangeMan is to reduce risk, which in turn saves money, as reflected by the downtime reductions...Without controls, the application life cycle is full of huge risks. Such risk is unacceptable, especially for regulated companies.” (May, 2003)

“According to clients interviewed, the single most important factor in selecting and using Serena ChangeMan is to reduce risk.”
—Robert Frances Group
May, 2003

Process-Oriented Change Management

Serena ChangeMan protects corporate assets by controlling every code change as illustrated in Table 2. It ensures that only successfully tested programs make it into production. Serena ChangeMan reduces maintenance costs and regression errors by moving code through an automated life cycle with accountability and quality assurance at every step.

Managed Processes	Automatically control and track all component processes.
Security	Protect your data in concert with your security system.
Impact analysis	Assess the ramifications of a change before it hits production.
Version control	An integral part of the streamlined process.
Library management	Manage any number of component versions.
Audit trails	Turn audits into routine activities.
Online approvals	Fast and secure, in parallel, serial or both.
Concurrent development	Eliminate overlays and cultivate developer communications.
Freeze control	Ensure that the changes tested are the ones put into production.
Automated backout	Revert to earlier code in seconds.
Checkout	Ensure developers are working with the right version every time.
Emergency protocols	Protect the integrity of the system while allowing quick fixes.

Table 2: Serena ChangeMan offers process-oriented change management

Issue Management

Serena TeamTrack is a process-centric issue management solution that provides enforcement down to the task level. It provides simple, flexible and powerful tools for mapping, tracking and enforcing business processes, as shown in Table 3. TeamTrack can be used to improve workflow, communication and accountability throughout the development life cycle.

Workflow Engine	Robust, multi-level hierarchical workflow engine links the overall business process with processes of department or groups
Management Dashboard	Full access to activity and resource status through comprehensive reports and charts
Ease of Use	Simple to design with built-in graphical workflow editor, and easy to use and administer
Integration with ChangeMan	Associate ChangeMan software code changes with a TeamTrack request
Accessibility	Web-based architecture provides authorized users with complete functionality over the Web

Table 3: Serena TeamTrack offers issue management

Satisfying Audit Requirements

By implementing Serena's application change management solutions, an organization can reduce the risk of non-compliance and ensure a well-managed application environment. Table 4 shows how Serena ChangeMan and Serena TeamTrack improve application life cycle management to help enterprises meet regulatory requirements.

CONTROL ITEMS	SERENA PRODUCT	CONTROLS
Initiation of change requests	TeamTrack	TeamTrack manages problems, issues, and change requests, and is integrated with ChangeMan.
Testing and approval of changes prior to migration into the production environment	ChangeMan	ChangeMan establishes a process where signoffs are required before any entity can be placed into production. Testing scripts can be initiated and verified in the test areas.
Critical calculations, data validations, exception routines, interfaces	ChangeMan	ChangeMan establishes a process where signoffs are required before any entity can be placed into production. Testing scripts can be initiated and verified in the test areas.
Job sequencing and relationships	ChangeMan	All jobs and their sequence can be verified before approval is given to place them into production.
Application migration procedures	ChangeMan	The integrity of the process and the access to applications and data during the process is managed by ChangeMan.
Backout processes	ChangeMan	Backout processes can be put into place with ChangeMan.
Validation of successful promotions to the production environment	ChangeMan	ChangeMan keeps an audit trail of all activities. All promotions can be verified through ChangeMan.
Emergency change procedures and processes	ChangeMan	As all movement to production is recorded in ChangeMan's audit log, emergency change procedures can be reviewed after the fact for their validity and appropriateness.
Documentation updated; user training completed	ChangeMan TeamTrack	Both ChangeMan and TeamTrack can manage documentation and training functions as part of the change process.
Segregation of duties	ChangeMan TeamTrack	Roles and responsibilities can be assigned with ChangeMan and TeamTrack.
Access to critical transactions and data	ChangeMan	Along with a security system, ChangeMan can limit access to application components to authorized individuals
Management of technical infrastructure	TeamTrack	TeamTrack can help with issue management.

Table 4: Serena ChangeMan, along with Serena TeamTrack, helps satisfy audit requirements

Navigating the Regulations

The following lists some of the regulations IT executives must navigate:

U. S. Public Company Accounting Reform and Investor Protection Act of 2002, known as the Sarbanes-Oxley Act

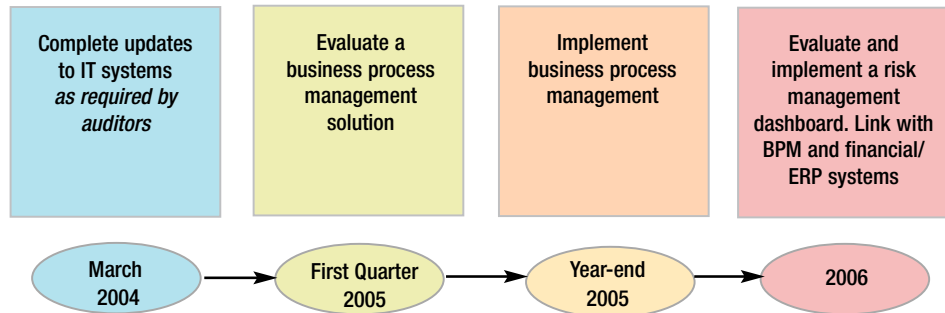


Figure 1: Sarbanes-Oxley Act Compliance Timeline

Source: Gartner, September 2003

The Sarbanes-Oxley Act, or SOA, creates new or enhanced standards for corporate accountability, along with penalties for wrongdoing. The timeline shown in Figure 1 outlines when organizations must comply with the act. Its intention is to reduce fraud and conflicts of interest while rebuilding public trust. The most significant sections for IT organizations are:

Section 302: Certification of Financial Reports

The CEO, CFO, and attesting public accounting firm must certify the accuracy of financial statements and disclosures. This requires that financial statements be complete and accurate.

Section 404: Management Assessment of Internal Controls

Section 404 is the most significant section for IT organizations, and the largest driver of Sarbanes-Oxley compliance. It requires a statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company. It also requires that the process used to generate financial statements be accurate and meet an accepted industry standard. As part of that framework, general computer controls will need to be implemented and documented.

Section 409: Material Event Reporting

This section requires enterprises to disclose information on material changes in financial conditions or operations on a rapid and current basis.

*"Proactive use of IT enables earlier detection and mitigation of material events."
— Gartner
September, 2003*

IT organizations play an important role as they support the enterprise's business operations and financial management. Most of the financial data used to produce financial reports is generated by applications managed by IT and its related processes.

Therefore it is critical these processes can be verified, and that IT executives can certify their reports come from managed software applications. Gartner states, "Although Sarbanes-Oxley doesn't directly regulate information technology, IT is the backbone of the financial processes that the law regulates. Therefore, the CIO will play a critical role in achieving compliance." And, "Proactive use of IT enables earlier detection and mitigation of material events."

(TG-21-0037 Sept. 25, 2003)

Gramm-Leach-Bliley Act (GLBA, or Financial Services Modernization Act of 1999)

This act requires that financial institutions certify their service providers are maintaining acceptable standards of client data protection. The certification process requires a definition of acceptable standards, creation of certification processes and instruments to meet those standards, and certification activity for each vendor.

California Security Breach Information Act (SB1386)

SB1386 seeks to reduce identity theft and protect California residents' right to privacy. It requires disclosure of any breach to the security of a computing system where there is a reasonable belief that an unauthorized person has acquired unencrypted personal information.

USA Patriot Act

One of its regulations is to regulate the activities of U.S. financial institutions, particularly their relations with foreign individuals and entities. It requires the availability of information across multiple systems to reveal patterns that indicate fraud and money laundering.

New Basel Capital Accord (Basel II)

This accord provides an operational risk management framework intended to encourage ongoing improvements in banks' risk assessment capabilities. To ensure the competitive balance, it proposes a capital standard for reasonable comparability across banks and across boundaries based on three pillars: capital standards, supervisory review, and market discipline.

U.S. Food and Drug Administration, Part 11 of Title 21 of the Code of Federal Regulations (21 CFR Part II)

This pharmaceutical project and process management regulation provides criteria for the agency to accept electronic records and electronic signatures as the equivalent of paper records and handwritten signatures.

U.S. Health Insurance Portability and Accounting Act (HIPAA)

HIPAA is a federal mandate that requires changes in healthcare record keeping. It seeks to streamline and standardize patient records and insurance claims by implementing record management standards throughout the U.S. healthcare industry.

U.K. Companies (Audit, Investigations and Community Enterprise) Bill

The U.K. government's proposals are designed to restore confidence in U.K. companies' auditing, accounting, and reporting. The measures require that directors state they have not held relevant information from their auditors, and it allows companies to be investigated if necessary.

ACT	Requirements	ChangeMan	TeamTrack
Sarbanes-Oxley	Section 404: General computer controls need to be implemented and documented	ChangeMan manages application changes across the enterprise providing appropriate audit trails. Code changes are monitored, documented, and approved.	TeamTrack manages business processes, problems, issues, and change requests, and facilitates communication among the appropriate team members. Business processes can easily be built and deployed, and TeamTrack can interface to ChangeMan.
GLBA	Financial institutions certify their service providers are maintaining client data confidentiality	ChangeMan places application software under its control. No unauthorized personnel can access this managed software for modification purposes.	
SB1386	Disclosure of unauthorized access to unencrypted personal information		
USA Patriot Act	Availability of information to reveal patterns that may preclude fraud and money laundering	ChangeMan manages application changes across the enterprise and makes available information about those changes to the appropriate authorized personnel.	
Basel II	Capital standards for reasonable comparability across banks and across boundaries	ChangeMan tracks and manages all changes made to software applications. It allows an organization to protect their existing application software, while managing the process of updating this software with any changes needed for compliance.	
21 CFR Part II	Accept electronic records and electronic signatures as valid		
HIPAA	Implement record management standards throughout the U. S. healthcare industry		
U.K. Companies	Directors state they have not withheld relevant information from auditors	ChangeMan manages application changes across the enterprise providing appropriate audit trails. Changes to code are monitored, documented, and approved. All information on program changes is readily available to the appropriate individuals.	

Table 5: How Serena products can help you with regulatory compliance

Case Study: A Practical Implementation of Serena Solutions

An organization deploys ChangeMan ZMF and ChangeMan DS to manage changes to software applications on various platforms across the enterprise. Working toward Sarbanes-Oxley compliance, Serena TeamTrack is deployed to help manage the business processes involved and any changes that are associated with these processes. Keeping complete documentation of who requested the change and their business need and all approvers of the change allows personnel involved to have the information they need, when they need it. With ChangeMan integration, a list of all the software elements effected by the change can be linked with a TeamTrack request.

Serena Software—A Trusted Partner

Serena is dedicated to providing superior value and exceeding customer standards. With more than 20 years of experience bringing innovative products to market, and more than 3600 customer sites, Serena has a proven track record of growth, profitability and stability, enabling continuous investments in new products and innovative solutions.

Contact

To learn more about Serena products and strategies, or to download your free, fully functional evaluation copy of Serena TeamTrack, visit Serena at www.serena.com or write us at info@serena.com.

serena[™] Automating Change

Serena, ChangeMan and TeamTrack are registered trademarks of SERENA Software, Inc. All other products or company names are used for identification purposes only and may be trademarks of their respective owners. Copyright © 2004 SERENA Software, Inc. All Rights Reserved. WP101_001_0104