

Business Mashups for Compliance

Are you compliant?

How much effort does it take?

What if...

...you could take an eight-week process and reduce it to eight hours

...with a solution that is implemented in 90 days

...and be ready for every future audit?

Business Mashups for Regulatory Compliance Reporting such as:

- Sarbanes-Oxley
- UK Combined Code
- Basel II
- HIPAA
- OCC/FED
- FISMA

The Compliance Challenge

Governance and control frameworks are becoming a part of IT management best practices to comply with ever-increasing regulatory requirements. Collecting evidence for IT audit is a time-consuming and manual process. For IT to successfully deliver against business requirements, management needs an internal control system – processes to automate the flow of approvals and change – as the most important aspect of audit readiness and a risk-based approach to management of the data environment.

Current Situation	The Opportunity
<ul style="list-style-type: none"> • Manual and unsecure evidence collection via “sneaker net” • Manual testing with visits and re-visits to control owners • Tracking testing and remediation activities in static files • Increasing complexity in IT risk and compliance in network security, privacy and financial reporting • Multiple regulatory requirements creates silos of control and audit information 	<ul style="list-style-type: none"> • Align IT with the company’s regulatory compliance requirements • Automate internal control review processes for easy replication and consistency • Reduce time spent recording and evaluating evidence for regulatory compliance • Serena Business Mashups generate audit evidence for security, change approval, development/acquisition, general IT controls and operations

The Mashup Solution

With security restrictions on networks and access to data, collecting evidence falls to the information technology department, management and staff. Every quarter, collection efforts can take 7 to 28 days – depending on the size of the organization and the number of auditors assigned. This evidence consists of documents, presentations, meeting minutes, system configuration settings, application configuration settings, security settings, change control information, user access requests, etc. – anything that affects the data environment.

The good news is that the collected data usually does not change locations, and the amount and type of data generated by systems are generally predictable in form and content. The data itself often contains the evidence required for an audit, so the collection and review of the evidence serves as the testing of the control. A Serena Business Mashup implementation takes advantage of these features to allow information technology auditors to collect data without dependence on the IT department.

How It Works

Sample Mashups

Compliance solutions to generate audit evidence:

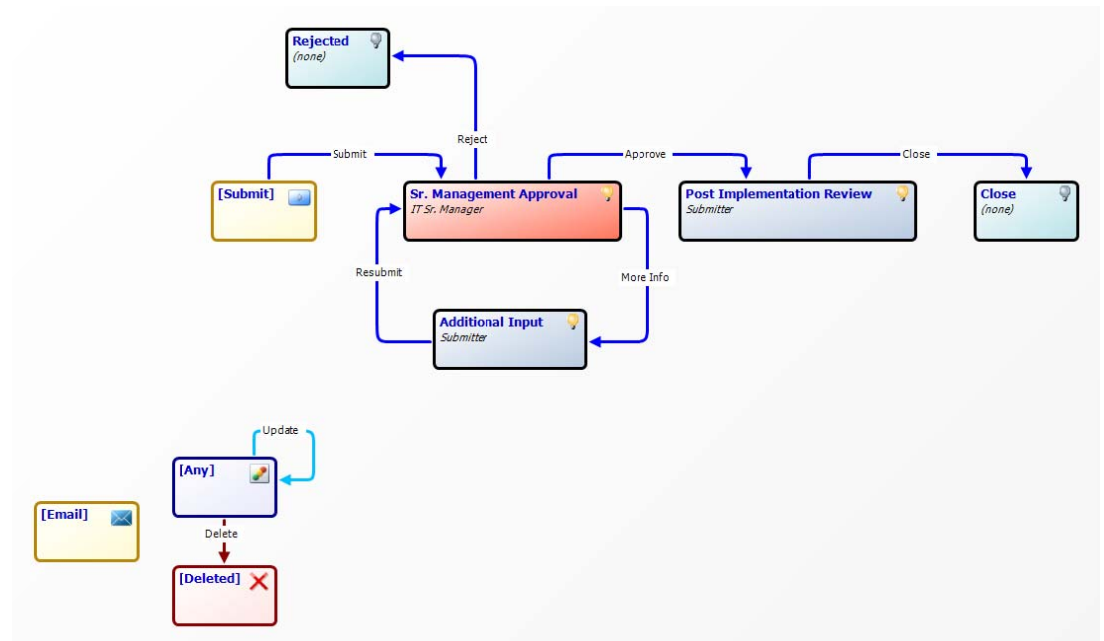
- Meeting Minutes Review
- IT Activity Review Process
- Job Description Review/Acceptance
- Employee Evaluation
- IT Training Form
- Data Integrity/Ownership
- Risk Management Workflow
- Emerging Technologies
- Incident Management Process
- Metrics Review Process
- Development/Acquisition
- Testing Review Process
- Change Approval Process
- Policy Review Process
- SDLC Process
- Emergency Change
- Batch Job Request Workflow
- Daily Operations Checklist
- Backup Issue Tracking
- Restore Request
- New Backup Request
- Existing User Access Change
- User Termination workflow
- Security Review Process
- Security Issue Tracking

Serena® Business Mashups enable users to create workflows, composite applications and Mashups that drive productivity by coordinating work across people and systems. For every project in IT, there are ten requests that never get addressed, contributing to an ever-growing application backlog and missed business opportunities.

Serena Business Mashups collect audit evidence through more than 25 processes for IT Operations. Evidence is gathered independent of any other application and resides completely in Serena’s process management product. Built using standard information technology workflow templates designed to the ITIL standard, it produces the evidentiary documentation required for the COBIT audit. With audit evidence gathering implemented as a Business Mashup, the annual audit activities no longer take 80+ hours to complete, and reduces the billing hours of the external audit firm.

Business Mashups for compliance generate audit evidence for security, change approval, development & acquisition, general IT controls and operations. Once collected in a manual review and approval processes, two thirds of an audit is automated. The audit process is a Business Mashup that recreates an audit trail for activities such as evidence gathering, audit reporting, control testing/reporting and remediation tasks – as a single business process workflow designed to manage all of the audit activities across many different locations or internal audit staffing configurations.

- Reduces testing execution timeline by 50-70%
- Allows for test reporting/dashboards
- Centralizes repository for testing data
- Reports represent the internal/external auditor’s documentation requirements



The Emergency Change Approval Mashup automates a process that ensures emergency change requests are authorized, documented and subject to formal change management procedures. It ensures that back-out procedures exist for all emergency changes before the change is made. **Who Participates:** Information technology staff required to make a change to the production environment and Senior Information Technology Management **Purpose:** All emergency changes are required to be documented and approved and evidentiary documentation is required to be produced for audit purposes.

Services For Audit Readiness And Remediation

Data, People, Process

The data gathered by Serena Business Mashups allows IT managers to report on rate of change in the production environment, chronic application or server problems, production issue trending, QA effectiveness, resources allocation and leveling, and development metrics. With Serena Business Mashups, technology managers can report metrics on even manual processes, forever changing the role of compliancy in information technology.

Serena Service Partner **fyoozhen+Consulting, Inc.** is a boutique firm specializing in regulatory compliance/audit services for information technology. They advise clients and develop business strategies to achieve compliancy in Sarbanes-Oxley, GLBA, Basel II, OCC/FED and FISMA regulatory conformity.

About Serena Software, Inc.

Serena provides services to make Enterprises and the business people within them more productive. More than 15,000 organizations around the world, including 96 of the Fortune 100, rely on Serena solutions delivered either on premise or on demand, to provide visibility and efficiency to the application development process. Serena is headquartered in Redwood City, CA, with offices throughout the U.S., Europe, and Asia Pacific. Visit us at www.serena.com

Services include comprehensive processes based on the COBIT methodology: Project Management, Change Management and IT Operations control domains. These semi-customized processes are configured to operate within the client's existing environment.

Regulatory Compliance Advisory Services for Information Technology

Assist IT departments with defining and implementing appropriate levels of controls and evidentiary documentation to complement the current operational processes – not replace it. We advise technology managers on control and narrative documentation, and deliver a targeted, well-defined operational framework to support continual maintenance for audit.

Technology Business Process Engineering and Review

Consult with technology departments to identify their current process, align the process with the appropriate departmental control and strategically design the resulting evidence insuring little room for misinterpretation from internal or external auditors.

Information Technology Department Advocacy

Educate internal and external auditors to ensure that they have a complete understanding of the controls implemented, the processes that were engineered to support controls and the purpose/meaning of the evidentiary documentation prior to the next audit cycle. Assist as an advocate to navigate complicated and often convoluted testing results and remediation requests – to preserve the operational framework of the IT department.

Information Technology Internal Assessment

Internal audit assessment services for companies whose internal audit teams require assistance or for companies without an independent internal audit function.

Information Technology Audit Framework Implementation and Review

Using the Control Objectives for Information Technology (COBIT) framework, we align the audit framework to the existing IT operational environment and deliver an audit plan consistent with published recommendations for audit readiness. The company's current audit framework is reviewed to identify weaknesses in the control or testing documentation and identify redundant controls and tests for a more efficient audit.

Multi-regulation Control Consolidation

Multiple regulatory requirements in an organization can create silos of control and audit information. Assists both the information technology and audit teams with identifying the overlapping controls and tests and developing a single IT audit and operational framework in support of all of the regulatory requirements.

Serena is a registered trademark of Serena Software, Inc. All other product or company names may be trademarks of their respective owners, and their use is intended for identification purposes only and not in association with or as sponsorship or endorsement by such owners.