



Streamlining Federal Mainframe Governance

A federal agency automates change governance to ensure compliance and stability with Rocket® ChangeMan®

COMPANY OVERVIEW

This US government agency operates and supports mission-critical systems for multiple agencies, underpinning essential functions such as financial processing and benefits administration. Their work reaches individuals nationwide, with special impact in rural communities.

CHALLENGE

Overcoming manual processes and strict audits

Operating in a highly regulated environment, the agency faces increased audit scrutiny, including FISMA (Federal Information Security Management Act), A123 (Office of Management and Budget Circular A-123), RMF (Risk Management Framework), and OIG (Office of Inspector General), requiring consistent governance and change control. They rely heavily on established

CHALLENGE

Relying on manual processes and specialized knowledge created compliance bottlenecks and increased operational risk.

IBM® z/OS® mainframe environments to support secure, stable systems of record. However, increasing pressure to modernize development practices without disrupting mission-critical operations led to inconsistent change management across teams and limited end-to-end visibility into software changes moving to production. Heavy reliance on manual processes and specialized tribal knowledge made audit preparation extremely time-consuming. As the workforce evolves, fewer experts are available to manage these complex environments, raising operational risk during peak processing periods.

SOLUTION

Centralizing control with Rocket ChangeMan

To establish a secure and auditable workflow across the agency's operations, Rocket ChangeMan was integrated directly into existing development and operational processes. This ensured live production systems were not disrupted while providing centralized, enforceable change governance with strict separation of duties and robust approval workflows. The platform captures a complete audit trail of all actions throughout the development cycle, from code checkout, to testing, approvals, and installation, detailing who completed each step and when. The component history database automatically tracks and manages compilation requirements for every element, freeing end users from needing to oversee technical specifics. In addition, a unique fingerprint is embedded in each production executable, which confirms that only authorized and properly reviewed components make it into production. Altogether, these features enable the agency to modernize confidently while maintaining operational security and integrity.

SOLUTION

The agency integrated centralized governance into current workflows, enabling seamless modernization without live system disruption.

RESULTS

Achieving faster compliance and system stability

The agency achieved significant reductions in their audit preparation efforts. Auditors can now use read-only access to run reports and verify compliance independently, freeing up internal staff. Operational consistency improved dramatically across all development teams, leading to increased confidence in production change integrity. By automating complex compilation rules, the agency reduced its dependency on individual knowledge holders. New developers and outside contractors can now focus entirely on writing code instead of navigating complicated operational policies. This streamlined workflow likely reduced errors in financial systems that impact numerous national programs. Looking ahead, the agency plans to explore integration with artificial intelligence tools to further automate component validation and rollback processes.



Audit efficiency

Read-only access empowers auditors to run independent reports, drastically reducing internal preparation time and effort.



Workforce enablement

Automated compilation rules allow developers to focus on writing code rather than memorizing complex operational procedures.



Production security

Unique executable fingerprints guarantee that unauthorized code cannot bypass the highly secure, established deployment process.

PRODUCT HIGHLIGHTS

Rocket® ChangeMan®

Key features

- Comprehensive audit trails track every action from development to deployment.
- Automated compilation management reduces errors and manual oversight.
- Executable fingerprinting ensures only authorized code reaches production.
- Seamless integration with GIT. GIT users are able to stay within a full GIT environment without needing to understand ChangeMan.

At a glance

- Automates approval workflows and enforces separation of duties.
- Simplifies audit prep and continuous compliance.
- Integrates with existing operations without disruption.



Modernization. **Without Disruption.**™

Visit RocketSoftware.com

[Explore more](#)

©2026 Rocket Software, Inc. or its affiliates. Rocket and the Rocket Software logos are registered trademarks of Rocket Software, Inc. Other product and company names may be trademarks™ or registered® trademarks of Rocket Software or its affiliates or their respective owners. Use of third-party trademarks does not imply any affiliation with, endorsement by, or association with Rocket Software.

IBM and z/OS are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

MAR-18067_LongUC_USGovernmentAgency_V4

