Rocket

COMPLIANCE

Sarbanes-Oxley Compliance with Rocket MultiValue

Public companies subject to Sarbanes-Oxley (SOX) legislation must document internal controls over financial reporting (ICFRs) related to their key financial reporting systems. Companies that perform development activities on these systems will need to demonstrate effective ICFRs for their development and change control processes to support the security and integrity of data within the financial systems. While every company defines the exact structure of its own ICFRs, certain expectations are common across any company performing development activities.

The Rocket® MultiValue Application Platform (Rocket MV), which includes Rocket UniData and Rocket UniVerse, offers robust security controls that enable companies to design and implement controls to comply with SOX requirements. Relevant (SOX) requirements, and the capabilities Rocket MV offers to address them, are listed below.

SOX Control Examples	Rocket MV Capabilities
Administrative system access is restricted to appropriate personnel.	All administration of user access and database security features is performed through a database management console, with access restricted to designated administrative users.
Access to the system and specific resources is restricted to individual users with a valid business need and authorization for such access.	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited only to authorized users. Rocket MV does not add or require any generic user accounts or default credentials.
Users attempting to access the system are authenticated during login.	User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). Rocket MV inherits all user access security controls you have implemented within your operating system credentials, including password construct requirements, account lockout for invalid login attempts, inactivity timeout, and disabling of dormant accounts.
User accounts and their associated access rights within the system are validated by an independent reviewer on a periodic basis.	Reports can be generated to show which users have access to specific data.
Changes to user accounts, access rights, or system parameters are reviewed by an independent reviewer on a periodic basis.	Audit logs can provide a secure record of any access or updates to user access rights, whether authorized or unauthorized.

Rocket
rocketsoftware.com
info@rocketsoftware.com
US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com