COMPLIANCE

Trust Services Principles for Service Organization Controls Reports with Rocket® Mainstar® Backup and Recovery Manager Suite

Service Organization Controls (SOC) reports are an effective way for companies to provide assurance to their customers and prospects about the security, availability, confidentiality, integrity, and privacy of the systems they offer. SOC 2 and SOC 3 reports are popular with Software-as-a-Service (SaaS) providers and any company with access to its customers' critical systems and data.

Each Trust Services Principle includes numerous criteria that must be satisfied by the service organization, as well as illustrative controls for how an organization may meet the requirements.

Rocket® Mainstar® Backup and Recovery Manager Suite (BRMS) centralizes your backup and recovery management processes for an IBM® z/OS® environment. With Rocket BRMS, you can be sure that all your critical datasets are being captured in your backup processes, and that those processes are actually occurring—essential controls both for satisfying your system availability commitments and for proving you are in an audit. Relevant SOC criteria, and the capabilities BRMS offers to satisfy them, are listed below.

CRITERIA	BRMS CAPABILITIES
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	BRMS operates within the security framework you have established for your systems. It leverages the logged-in user credentials of the native IBM TSO function. TSO credentials, and all authentication mechanisms tied to that login, are inherited by BRMS. IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. BRMS functions validate that the user has SAF rights and cannot bypass mainframe access restrictions.
CC5.3 Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	BRMS does not have a dedicated set of system user credentials. Instead, it leverages your TSO credentials and all associated authentication mechanisms. There are no separate user credentials for or within BRMS.
CC5.4 Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.	IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. BRMS functions validate that the user has SAF rights and cannot bypass mainframe access restrictions. All relevant changes to user accounts, roles, and assigned permissions through the SAF are fully logged through the IBM System Management Facility (SMF). Reporting and alerting on such actions can be configured through the mainframe functions. All actions performed through BRMS against backup jobs and datasets are traceable to individual users executing the function. Detailed logging is available through the IBM Resource Access Control Facility (RACF).

CRITERIA	BRMS CAPABILITIES
A1.2 Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.	BRMS is designed to help you address this need. It performs analyses to identify all critical datasets and determine whether they're included in your backup processes, or whether they're omitted or outdated. BRMS provides a centralized management interface to configure, monitor, and report on the various predefined backup jobs executed by all your backup software for the entire IBM z/OS environment. Interfaces with your backup software allow BRMS to generate backup jobs to cover any missing data sets. Reporting functionality shows the status of each dataset and each backup or restoration task, to ensure successful completion. Backup collection logs and reports are retained with BRMS to maintain historical evidence for auditors and examiners.
A1.3 Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	BRMS automatically generates jobs to restore data sets that can be used for periodic testing requirements. Restoration jobs are customized to include the datasets specifically required to restore a given application.
PI1.1 Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	BRMS monitoring of backup job status allows you to identify errors that could result in compromised data integrity of your backup volumes.
PI1.4 Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	Backup logs and reports are retained with BRMS to maintain historical evidence for auditors and examiners. Where backup jobs are intended for archival of historical data, BRMS proves that all such datasets are included in your processes and their backup jobs are successfully executed without errors.

CRITERIA	BRMS CAPABILITIES
C1.2 Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality requirements.	BRMS enhances the capabilities of native ABARS facilities to ensure that restored files cannot have modified security permissions, protecting the confidentiality within the restored files. TSO and SAF enforce data access restrictions for any user in the system. BRMS cannot bypass these permissions.

Rocket

rocketsoftware.com
info@rocketsoftware.com
US: 1 855 577 4323
EMEA: 0800 520 0439
APAC: 612 9412 5400
twitter.com/rocket
www.linkedin.com/company/rocket-software
www.facebook.com/RocketSoftwareInc
blog.rocketsoftware.com