COMPLIANCE

Trust Services Principles for Service Organization Controls Reports with Rocket® OpenTech

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.

The Rocket® OpenTech portfolio includes Rocket DR/Xpert, Rocket DASD Backup Supervisor, Rocket Tape/Copy, Rocket Virtual Data Recovery, and Rocket CopyExport Manager. These products provide you with all the tools you need to implement a strong backup management program and availability controls for your entire IBM® z/OS® environment—from executing backup and migration jobs, to monitoring job statuses, to simulating restoration events, and more. Relevant SOC criteria, and the capabilities OpenTech products offer to satisfy them, are listed below.

CRITERIA	OPENTECH 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.	OpenTech products leverage the logged-in user credentials of the native IBM TSO function. TSO credentials, and all authentication mechanisms tied to that login, are inherited by all OpenTech products. IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. OpenTech product functions validate that the user has SAF rights and cannot bypass mainframe access restrictions. While features such as Tape/Copy's tape browse function allow access to data within backup volumes, this access is still restricted by the SAF permissions for the logged in user.
CC5.3 Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	OpenTech products leverage your TSO credentials and all associated authentication mechanisms. There is no need to maintain a separate user account list for any OpenTech products.
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.	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 OpenTech products 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).
CC5.7 The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability, processing integrity, or confidentiality.	DR/Expert, DASD Backup Supervisor, and Tape/Copy products leverage the Integrated Cryptographic Services Facility (ICSF) to protect backup data during transit between storage locations. They can also support RSA encryption for this function.

CRITERIA	OPENTECH CAPABILITIES
A1.1 Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.	DASD Backup Supervisor stacks backup volumes to minimize tape usage and maximize storage capacity.
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.	DR/Xpert helps analyze production batch jobs and datasets automatically to identify those that are critical, and continuously monitor for changes. It can then ensure that all critical datasets have backed-up or mirrored datasets available, and tell you where those copies are. DR/Xpert centrally manages your backup utilities (such as Tape/Copy) to automatically generate backup jobs—as well as restoration jobs when they're needed—and integrates them with your job scheduling. DASD Backup Supervisor continuously monitors for new or modified volumes and maintains backup jobs to ensure that they are reliably backed up. Tape/Copy executes the backup process from tapes to other media, and builds in error reporting and recovery features to ensure all your data volumes remain intact. DR/Xpert provides facilities in the event of a disaster recovery incident for managing restoration tasks, and allows prioritization of recovery according to your RTOs. Combined with the storage and recovery efficiency features of the other OpenTech products, this helps you minimize system downtime in a recovery event.
A1.3 Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	DASD Backup Supervisor generates automated recovery jobs associated with its backup tapes to be stored alongside the data. This allows for quick, simple, and efficient restoration in a test or a real disaster recovery scenario. DR/Xpert monitors backup data for all critical datasets to ensure you are within your Recovery Point Objective (RPO) windows.

CRITERIA	OPENTECH CAPABILITIES
PI1.1 Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	Tape/Copy integrates data validation controls to detect any errors in the conversion process, preventing any data integrity issues from being transferred to the new media. CopyExport Manager enhances the capabilities of the native copy export process by adding automatic error detection and reporting for archival of your critical data sets from virtual tape libraries to physical tapes.
PI1.4 Data is stored and maintained completely and accurately for its specified life span in accordance with processing integrity commitments and requirements.	DR/Xpert identifies all critical data, or enables you to view data by other categories such as department or application, to help ensure that adequate backups are being performed on the selected data. Backup logs and reports are retained with DR/Xpert to maintain historical evidence for auditors and examiners. For data volumes in your virtual tape library, Virtual Data Recovery automatically detects data differentials and backs them up for archival to a consolidated medium for efficient storage and restore ability.
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.	IBM Security Authorization Facility (SAF) provides standard access controls over data based on the TSO login. OpenTech functions validate that the user has SAF rights and cannot bypass mainframe access restrictions. While features such as Tape/Copy's tape browse function allow access to data within backup volumes, this access is still restricted by the SAF permissions for the logged in user.

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