COMPLIANCE

Trust Services Principles for Service Organization Controls Reports with Rocket Aldon Lifecycle Manager

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/or 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 a number of criteria that must be satisfied by the service organization, as well as illustrative controls for how an organization may meet the criteria.

Rocket® Aldon Lifecycle Manager (Aldon LM) has robust security controls available to enable a company to design and implement controls to achieve the Trust Services Principles and their associated criteria. Relevant criteria, and the capabilities Lifecycle Manager offers to achieve each criterion, are listed on the following pages.

TRUST SERVICES CRITERIA	ROCKET ALDON LIFECYCLE MANAGER 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.	Aldon LM and its associated modules (LM(u), LM(e), Community Manager (Aldon CM), and Security Server) support unique user IDs for all individuals accessing the systems. Passwords are required for users to access each system. Aldon LM also supports integration with IBM i user credentials, and Aldon CM supports LDAP integration with Active Directory credentials. Detailed, customizable role-based access levels let an organization define the exact capabilities of each system user. Permissions are granular to support any organization's business needs according to the rule of least privilege and segregation of duties. Reports are available showing all users with their associated access capabilities.
CC5.2 New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	System administration is performed through the separate Security Server module, with access restricted to designated administrative users. Aldon CM module supports automated, system-driven workflows that may include access request, authorization, and provisioning processes. Workflows can be assigned to Security Service Manager administrators for Aldon LM, as well as administrators for any other system in use at an organization. The Aldon CM module can also support workflows for termination and offboarding processes that include the removal of system access that is no longer needed. Reports are available showing all administrative activity performed within the system, including the modification of user access and roles.
CC5.3 Implement a security awareness and training program for all members of its workforce (including management).	Passwords are required for all users attempting to log into the systems. Local credentials are stored in encrypted hash format on the Security Server service. Aldon LM(i) integrates with IBM i credentials, and Aldon CM offers LDAP integration with Active Directory credentials.
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.	Aldon LM users are assigned to role-based access levels for each development project. Administration of users and their roles is performed through the separate Security Server module. Roles are customizable to meet an organization's specific controls requirements.
CC5.5 Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations as well as sensitive system components within those locations) is restricted to authorized personnel.	Systems are installed on premises, and the organization can implement physical and environmental controls as with all other computing equipment.
CC5.6 Logical access security measures have been implemented to protect against security, availability, processing integrity, or confidentiality threats from sources outside the boundaries of the system.	Systems are installed on premises, so the organization's perimeter network security will cover LM systems.
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.	Users access the web-based Aldon LM(e), Security Server, and Aldon CM systems using encrypted HTTPS sessions. LM(i) utilizes encrypted SSH sessions. All data in transit—including code being checked in or out, or moved to new environments—is encrypted.

TRUST SERVICES CRITERIA	ROCKET ALDON LIFECYCLE MANAGER CAPABILITIES
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security, availability, processing integrity, or confidentiality commitments and requirements.	Aldon CM supports workflows for changes and development activities such as requests, approvals, testing, acceptance, and any other stages required by an organization's policies. Aldon LM supports multiple development environments that are customizable by the organization, such as development, test, staging, and production. Access for individual users to access, modify, or approve code can be assigned for specific projects, release versions, and environments. Developers can be restricted from making changes to software in testing or production. The ability to migrate between development, test, and production environments can also be restricted to appropriately segregated users. All actions within Aldon LM and its associated modules, including code changes and promotions, are fully logged and reportable. Changes made to code are highlighted by the Harmonizer module, which supports formal, independent reviews of code changes before promotion to ensure that changes are in accordance with an approved work order. Emergency changes can be allowed, but this requires approval of a
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.	Systems are installed on premises, and the organization can implement physical and environmental controls as with all other computing equipment.
PI1.6 Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Access to modify data is restricted to users specifically authorized within that development release and environment. The Harmonizer module highlights all changes made to code, allowing the organization to validate that all changes were made in accordance with an approved work order.
C1.1 Confidential information is protected during the system design, development, testing, implementation, and change processes in accordance with confidentiality commitments and requirements.	User access to various environments, such as development, testing, staging, or production, can be individually restricted.
C1.2 Confidential information within the boundaries of the systems protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality requirements.	Role-based access levels define each user's specific capabilities for accessing and/or modifying data within the system. All actions performed within the system, including accessing or modifying data, are logged and auditable.

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