![RACKTOP logo]

Risk Management Framework (RMF)

Compliance requires implementation of controls, continuous monitoring, and enforcement, as well as evidence of controls and enforcement.

RMF Overview

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions
- Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e. common controls)

BrickStor SP Maps to All Revelant Areas of RMF

Example Controls from NIST 800-37, 53, 137

Access Controls – Account Management, Least Privilege, Atypical Usage, Access Enforcement, Information Flow, Support for Attribute Based Access Control (ABAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC), Mandatory Access Control (MAC)

Audit and Accountability – Content of Audit, Audit Storage Capacity, Timestamps,Review and Analysis, Reduction and Reporting

Configuration Management – Access Restrictions, Signed Software Updates

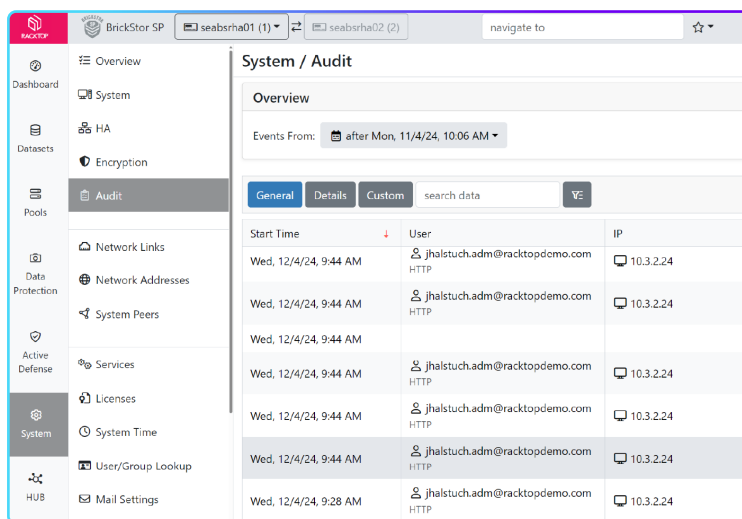**Contingency Planning** – Information System Recovery and Reconstitution

Identification and Authentication – Device Authentication, Authentication Management, Authentication Feedback
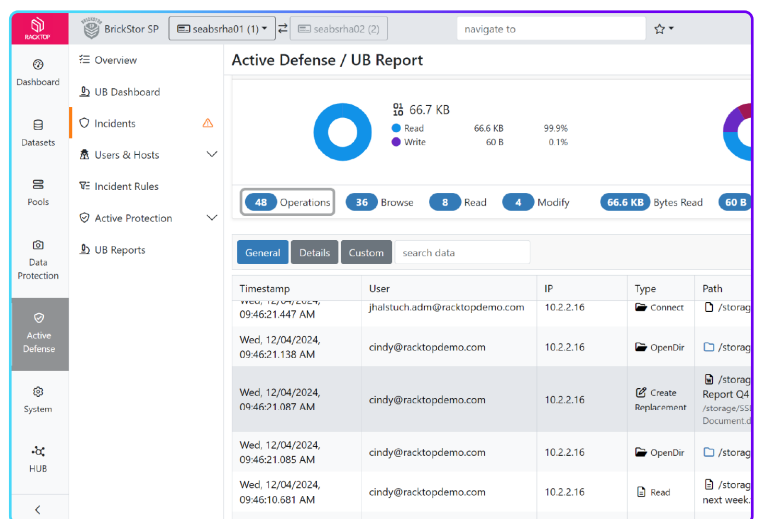
Media Protection – Media Sanitization

System and Communications Protection – Security Function Isolation, Cryptographic Key Establishment and Management, Cryptographic Protection, Transmission Confidentiality and Integrity, Protection of Information at Rest

System and Information Integrity – Software Firmware Integrity, Information Handling and Retention

Integrated compliance reports demonstrate ongoing evidence of controls and compliance

Audit Report

User Behavior Analysis