# RACKTOP

# **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; and
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e. common controls).

•	•					
RACKTOP	BrickStor SP	na02 (2) ▼ → seabsrha01 (1) navigate to	☆ •			
Ø	Æ Overview	<b>e</b>				
Dashboard	🕒 UB Dashboard	General		Contents		
₿	O Incidents	ID INC-RT0000BE-1387		General		
Datasets	ੈ & Users & Hosts ∨	Behavior / Threat Level         Unusual Access/Off Hours Access         3           User         & ccharette.adm@racktopdemo.com		Access Control Impacted Files and Recommendations		
	ম্ট্র Incident Rules	IP 📮 10.2.19.17 Hostname 📮 ChrisJumpBox3.racktopdemo.com.		Notes		
Pools	${igodot}$ Active Protection ${}{$	Datasets p02/global/chris-share		History		
<b>ਹਿ</b> Data	🕒 UB Reports	Snapshots Snapshots not held Watchers	Edit Watchers			
Protection		• • •				
		Detected Acknowledged Restore Acces Tue, 10/22/24, 10:22 AM Wed, 10/23/24, 10:22 AM auto-remediate	s Incident Closed Wed, 10/23/24, 10:22 AM auto-remediate			
<b>©</b> System		Access Control				
		2 ccharette.adm@racktopdemo.com	Not Blocked $2 - \checkmark \rightarrow \square$			
+X HUB		<b>—</b> 10.2.19.17	Not Blocked $\Box - \checkmark \rightarrow \square$			
		Incident closed. Open another incident to block user/host.				
<		anal gaad 0 ana	in time			

## BrickStor SP Maps to All Relevant 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), and 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

•														
NOTE:	BrickStor SP 🔳 seab	srha02 (2) ▼ ₹ 🖾 seabsrha01	11 (1) navigate to	合 *			-;¢: @							
0	Active Defense / Unusual Access/Off Hours Access						₽							
shboard	D UB Dashboard	General				Contents	î							
Pools	<ul> <li>◯ Incidents</li> <li>▲ Users &amp; Hosts</li> <li>✓</li> <li>▼E Incident Rules</li> <li>⊘ Active Protection</li> <li>✓</li> <li>▲ UB Reports</li> </ul>	ID Behavior / Threat Level User IP Hostname Datasets Snapshots Watchers	INC.R100008E-1397 Unusual Access/Off Hours Access ( ) () () () () () () () () () () () () () (	Edit Wated		General Access Control Impacted Files and Rec Notes History								
Ø		Detected	Acknowledged Restore Acces	ss Incident Closed	MONTO	🗑 BrickStor SP 🔳	J seabsrha01 (1) ▼	navigate to		<b>☆</b> ▼			*	
Active Defense		Tue, 10/22/24, 10:22 AM		Wed, 10/23/24, 10:2 AM	2 ≡	Active Defense /	UB Report				Rerun Remove	All Reports	ts €	
verense			auto-remediate	auto-remediate	扫	p01 💥 Raw Operat	tions : Newest to Oldest							
System Access Control				Read and Modify Main Datasets										
						Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signal Active Delete   Rename         Image: Signal Active Delete   Rename           Image: Image: Signa								
нив		Q 10.2.19.17		Not Blocked 📮 — 🗸 –										
		Incident closed. Open anot	other incident to block user/host.		¥5	Overview							sho	
<			ممعالمما المعر	in-teres	0	General Details	Custom search data							
					₽	Timestamp	User	IP	Туре	Path		Bytes	Sta	
Audit report						Sat, 10/05/2024, 12:07:40.053 PM	jhalstuch.adm@racktopdemo.com	10.2.2.16	Read	/storage/p01/global/eagle/01_Rackter zontal.png	op_LogoRGB_FullColor_H	ori 238.8 KB	0	
						Sat, 10/05/2024, 12:07:39.723 PM	cindy@racktopdemo.com	10.2.2.16	Read 4x	/storage/p01/global/eagle/01_Rackter zontal.png	op_LogoRGB_FullColor_H	ori 138.8 KB	0	
					Sat, 10/05/2024, 12:07:39.103 PM	cindy@racktopdemo.com	10.2.2.16	Read 3x	/storage/p01/global/Project X35/F22	2-1.mp4	1 MB	0		
						Sat, 10/05/2024, 12:07:38.706 PM	cindy@racktopdemo.com	10.2.2.16	Read 2x	/storage/p01/global/Project X35/F22	?-1.mp4	264 KB	0	
						Sat, 10/05/2024, 12:07:36.903 PM	cindy@racktopdemo.com	10.2.2.16	Read	/storage/p01/global/eagle/GigaOM.	txt	13 B	0	
					>	Sat, 10/05/2024, 12:07:36.872 PM	jhalstuch.adm@racktopdemo.com	10.2.2.16	Read	/storage/p01/global/eagle/GigaOM.	txt	26 B	0	

User behavior auditing