BOCADA

Fulfilling SOC 2 Compliance With Bocada

Developed by the American Institution of CPAs, the Service Organization Controls (SOC) is a way for companies providing services like data hosting, colocation, and data processing a way to prove their resilience and operations standards. Of particular interest to data protection and recovery professionals is the SOC 2 Report, an audit process indicating a data service company's compliance with SOC's five Trust Services Principles of security, availability, processing integrity, confidentiality and privacy.

As a centralized, automated governance reporting solution, Bocada offers organizations an efficient, streamlined approach to demonstrating SOC 2 compliance. By unifying backup activity data from complex hybrid-cloud environments under a single pane, Bocada gives backup, storage and regulatory teams a core tool to satisfy SOC 2 reporting guidelines.

Security Policies: The entity defines and documents its policies for the processing integrity of its system

SOC Guidelines	How Bocada Supports The Performance Monitoring Rule
1.2b The entity's system processing integrity and related security policies include...retention and destruction requirements.	Data retention policy reporting provides audit trails to verify data is kept for as long as needed and was purged when required.

Procedures: The entity placed in operation procedures to achieve its documented system availability objectives in accordance with its defined policies

SOC Guidelines	How Bocada Supports The Performance Monitoring Rule
3.1 Procedures exist to (1) identify potential threats of disruptions to systems operation that would impair system availability commitments and (2) assess the risks associated with the identified threats.	Built-in SLA compliance reporting simplifies demonstrating adherence to backup success rates, retention policy enforcement and other necessary backup activities.
3.2 Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable	Automated backup performance reporting identifies failed backups, enabling tailored troubleshooting so data is always protected and restorable.
3.3. Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	In-progress backup job reporting across hybrid-cloud environments allows processors to proactively address issues that could harm data restoration.
3.4 Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.	VM Analysis Reports allow enterprises to identify machines that are not being protected by their backup software so that non-backup issues can be corrected.
3.10 Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	Automated compliance report creation, scheduling and distribution offers a recurring governance process for reviewing backup fidelity and sharing compliance status with internal and external auditors.
3.12 Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Ticketing systems integration allows for automated creation of service tickets and faster notification and resolution.
	Built-in critical failure alerting enables processors to address data backup failures quickly so that valuable data is protected.
	Annotations make it easy to permanently document variances and audit steps taken to fix backup failures to protect data security.

Monitoring: The entity monitors the system and takes action to maintain compliance with its defined system security policies	
SOC Guidelines	**How Bocada Supports The Performance Monitoring Rule**
4.1 The entity's system security is periodically reviewed and compared with the defined system security policies. *4.3 Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis and policies are updated for that assessment.*	Bocada automates pulling and normalizing backup data across geographies, departments, and business units on a recurring basis, allowing for periodic reviews of the entire backup environment. Bocada offers reporting on over 20+ on-prem and cloud backup products, providing complete oversight even as organizations pursue digital transformation initiatives.

To assess your SOC 2 compliance readiness, try Bocada in your backup environment.

CONTACT US AT:
sales@bocada.com
or 425-898-2400