ComplyScan Plus (CS/P)

AWS Customers are in constant search of simple and easy ways to achieve compliance and improve their resiliency in a Disaster. AWS Storage services, together with AWS Backup provide fully managed services for AWS customers to optimize their restore and recovery capabilities in the cloud. *ComplyScan Plus* (CS/P) increases these AWS capabilities by plugging into these native AWS services to deliver validation, testing and visualization for AWS customers worldwide. The result is a new experience when using AWS services, with increased automation, scalability and simplicity.

CS/P can help you to achieve optimal velocity when using AWS services. CS/P provides AWS Backup visualization, threshold alerting, notifications, Slack integration and cross-account/cross-region snapshot validation to help better manage your FINRA, HIPPA, ISO, NIST and other regulatory compliance for your RPO/RTO requirements.

ComplyTrust Inc….AWS Partner helping AWS customers enhance recovery, restore and compliance capabilities

Data Sheet

Critical New Controls

Control name	Control description	Customizable parameters	AWS Config recording resource type	AWS Backup Audit Manager	CP/S
Snapshot Validation	Validates snapshot integrity and viability to achieve RPO/RTO/SLA	Accounts, Regions, Services, Zones	AWS Backup: backup selection		√
Backup Testing	Evaluates if backup testing is being done which is critical to NIST and other security frameworks	Accounts, Regions, Services, Zones	AWS Backup: backup selection		√
Snapshot Cost	Evaluates snapshot resource costs	Accounts, Regions, Zones	AWS Backup: backup selection		√
Snapshot activity	Monitors and Reports all AWS Backup on-demand and scheduled activity	Accounts, Regions, Users, Zones	AWS Backup: backup selection		√
Visualization	Dashboard with graphical representation of status, thresholds, and alerts	Accounts, ARN, Date, Regions, Services, Users, Zones and more	AWS Backup: backup selection		√
Backup resources protected by backup plan	Resource protected by a backup plan	Resources/ Recovery Points	AWS Backup: backup selection	√	√
Backup plan min-frequency and min-retention	Backup frequency setting at least [1 day] and retention period is at least [35 days]	Backup frequency; retention period	AWS Backup: backup plans	√	√
Backup prevent recovery point manual deletion	Backup vaults and recovery points undeletable except by AWS Identity and Access Management (IAM) roles	Up to 5 IAM roles that allow manual deletion of recovery points	AWS Backup: backup vaults	√	√
Backup recovery point encrypted	Encrypted recovery points	Resources/ Recovery Points	AWS Backup: recovery points	√	√
Backup recovery point minimum retention	Recovery point retention period set to at least [35 days]	Recovery point retention period	AWS Backup: recovery points	√	√
Cross-Region copy	Resource configured to create copies of its backups to another AWS Region	AWS Region	AWS Backup: backup selection	√	√
Cross-account copy	Cross-account backup copy configured	AWS account ID	AWS Backup: backup selection	√	√
Backup Vault Lock	Resource configured to have backups in locked backup vault	Min Retention Days; Max Retention Days	AWS Backup: backup selection	√	√

ComplyTrust®
Data Compliance & Privacy