



SOC 2 Compliance In The Cloud



SOC 2 Compliance

SOC 2 is a reporting framework that defines security criteria for managing client data and is developed by the American Institute of CPAs (AICPA). Teams can use SOC 2 reports to validate security efforts to clients and partners.

Set SOC 2 Administrative Security Policies

Organizations can utilize Dash ComplyOps to develop a set of custom administrative policies and standard operating procedures (SOPs) design around the latest AICPA SOC 2 2017 Trust Service Criteria. Each policy is mapped to SOC 2 security standards. Policies address topics including:

- Security Roles
- Risk Assessment & Risk Analysis
- Disaster Recovery
- Employee Training
- System Access
- Configuration Management
- Incident Response

Enforce Policies and Internal Controls

Dash enables teams to enforce set administrative policies and manage SOC 2 internal security controls through continuous compliance monitoring. Dash automatically scans and monitors your cloud environment and security settings for compliance issues including:

- Encryption
- Access Control
- Backup
- Network & Firewall Rules
- Audit Logging
- Intrusion Detection

☰ Compliance Center 👤

Priority	Name	Assigned To	Account	Source	Service	Items	Date	
Medium	Subnet(s) with allow all ingress NACLs		AWS Account	scan	vpc	71	2 months ago	Issue Status
Medium	Subnet(s) with allow all egress NACLs		AWS Account	scan	vpc	71	2 months ago	Issue Priority
High	S3 Bucket(s) have access logging disabled		AWS Account	scan	s3	56	3 months ago	AWS Accounts
Medium	Subnet(s) detected without a flow log	NH	AWS Account	scan	vpc	53	3 months ago	Source
High	EC2 Security Group(s) opens SSH port to all	NH	AWS Account	scan	ec2	51	3 months ago	



Conduct SOC 2 Audit

After implementing Dash administrative and technical controls, teams can engage with our third-party SOC 2 auditing partner or an independent auditing firm to go through a SOC 2 audit. A SOC 2 auditor will assess internal controls and provide a SOC 2 Type I or SOC 2 Type II audit on after security evaluation. Dash security controls and compliance management platform make it easy to work with auditors and streamline assessment.

Maintain SOC 2 Controls

Security teams can leverage Dash Compliance Reports to see the latest inventory and status of SOC 2 security controls. Organizations can utilize Dash compliance monitoring to detect any SOC 2 issues and maintain SOC 2 security controls during and after a SOC 2 audit.

The screenshot displays the 'Report Center' interface. At the top, there is a 'Report Center' header with a menu icon. Below it is a green bar labeled 'Framework Control and Controls Mapping' with a 'Back' button. Underneath, there are 'Collapse All' and 'Expand All' buttons. The main content area is divided into two sections: 'Control Environment' and 'Communication and Information'. The 'Control Environment' section lists four controls, each with a green status indicator: CC1.2 - COSO Principle 2, CC1.3 - COSO Principle 3, CC1.4 - COSO Principle 4, and CC1.5 - COSO Principle 5. The 'Communication and Information' section lists one control: CC2.1 - COSO Principle 13. Each control description is truncated with an ellipsis.



Cloud Compliance Expert

Dash is developed and supported by cloud security and compliance experts. We help organizations automate compliance standards including SOC 2, HIPAA, HITRUST, and NIST 800-53, and realize the true power and flexibility of the public cloud. Dash has built around the compliance needs of market-leading cloud providers and is an **AWS Advanced Technology Partner** and **Healthcare Competency Partner**.

Learn how [Dash ComplyOps](#) enables teams to achieve SOC 2 type 2 in the public cloud.

