SOC 2 Compliance with Apono Just-in-Time Cloud Access Platform

System and Organization Controls 2 (SOC 2) regulations address challenges related to securing systems, protecting sensitive data, and ensuring operational integrity in service organizations.

They focus on safeguarding customer information against unauthorized access, breaches, and misuse while promoting accountability and transparency. SOC 2 also helps organizations manage risks, maintain trust, and demonstrate compliance with best practices in data protection and service reliability.

Apono JIT Benefits to SOC 2 Compliance

Enforcing Least Privilege
Limiting access to only what is necessary for specific tasks and revoking it afterward.

Enhancing Auditability
Creating detailed logs of access activities for transparency and compliance.

Protecting Sensitive Data
Reducing risks of unauthorized access or prolonged exposure to confidential information.

Apono's Just-in-Time (JIT) access solutions align with several specific requirements of **SOC 2** by ensuring secure, controlled, and auditable access to sensitive systems and data. Continuous monitoring and auditing ensures that every access request is logged, and accountability is maintained across systems. Reporting is easily exportable in a protected PDF for assured compliance.

Mapping Apono Capabilities to System and Organization Controls 2 (SOC 2)

SOC 2 Requirement	Apono Security Control
Security: Access Control	
CC6.1 Logical access security measures are used to restrict access to authorized personnel.	Provides temporary, task-based access to systems, ensuring only authorized individuals can access sensitive data.
CC6.2 User access is managed based on roles and responsibilities.	Dynamically provisions access according to predefined roles and IAM context, ensuring adherence to the principle of least privilege.
CC6.3 User access is revoked when no longer needed.	Automatically revokes access after a predefined time or task completion, reducing risks from standing privileges.

Confidentiality: Protecting Data	
CC7.1 Procedures are in place to monitor system components and detect unauthorized access.	Logs and monitors all access activities, providing a clear audit trail for compliance and detecting anomalous access attempts.
CC7.2 Confidential information is protected during storage and transmission.	Restricts access to sensitive data to only when required, minimizing unnecessary exposure during storage and use.
Privacy: Limiting Access to Personal Data	
CC8.1 Personal information is collected, retained, and disclosed in accordance with the organization's privacy commitments.	Ensures temporary, purpose-based access to personal data, aligning with privacy commitments.
Auditability and Accountability	
CC6.6 Activities of authorized users and the use of system resources are logged.	Maintains comprehensive logs of who accessed what, when, and why, simplifying audits and providing evidence for compliance.
CC9.2 Security incidents are reported, logged, and addressed.	Reduces the risk of incidents by limiting standing privileges and providing actionable logs for incident investigation.
Risk Management	
CC3.2 Risk assessments consider potential threats and vulnerabilities.	Reduces the attack surface by eliminating standing access and dynamically granting access only when needed.
CC3.3 Identified risks are mitigated with appropriate controls.	Implements proactive access control measures to mitigate risks associated with unauthorized access.
Availability: System Availability and Performance	
CC5.1 System components are monitored to identify anomalies or potential performance issues.	Ensures secure, monitored access to critical systems, reducing downtime caused by misuse or mismanagement.

About Apono

Founded in 2022 by Rom Carmel and Ofir Stein, Apono is redefining cloud security with its Cloud Privileged Access Platform. With decades of expertise in cybersecurity and DevOps, Apono enables organizations to adopt just-in-time, just-enough privilege access, seamlessly bridging the gap between security and engineering teams. Trusted by Fortune 500 companies, Apono's platform empowers enterprises to enhance operational efficiency while maintaining robust security controls. Recognized in Gartner's Magic Quadrant for Privileged Access Management for two consecutive years, Apono is at the forefront of innovation in secure cloud access management.

APONO

www.apono.io

@Apono_official

@aponoio