




# NIST Compliance with Apono Just-in-Time Cloud Access Platform




**National Institute of Standards and Technology (NIST)** regulations address challenges such as ensuring the confidentiality, integrity, and availability of information systems, mitigating cybersecurity risks like unauthorized access, data breaches, and insider threats. They promote robust access control, identity management, and implementation of the least privilege principle.




## Apono JIT Benefits for NIST Compliance

-  **Limits Privilege Escalation**  
Reduces risks associated with permanent admin or elevated access roles.
-  **Improves Auditability**  
Simplifies tracking and reporting for compliance.
-  **Supports Zero Trust**  
Enhances access control strategies by dynamically adapting permissions.

Apono's Just-in-Time (JIT) access solutions enable organizations to maintain compliance, streamline incident response, and enhance risk management for evolving cyber threats. 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 NIST Cybersecurity Controls

NIST Requirement	Apono Security Control
 <u>NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations)</u>	
<b>AC-2 (Account Management)</b>	Apono's JIT access ensures that accounts and permissions are managed dynamically, reducing unnecessary standing privileges and aligning with proper account creation, use, and revocation.
<b>AC-6 (Least Privilege)</b>	Apono supports enforcement of the principle of least privilege by granting permissions only for the duration and scope required, preventing excessive or unnecessary access.
<b>AC-19 (Access Control for Mobile Devices)</b>	JIT access can enforce time-bound and task-specific access for mobile device users to prevent unnecessary risks.

<b>AC-17 (Remote Access)</b>	Apono enables organizations to enforce restrictions for remote access, ensuring access is time-limited and used only for specific purposes.
<b>AU-12 (Audit Record Generation)</b>	JIT access solutions often integrate logging and auditing, which help meet requirements for generating detailed logs for access-related events.
 <b>NIST Cybersecurity Framework (CSF)</b>	
<b>Protect Function</b>	
<b>PR.AC-1 (Identity Management and Access Control)</b>	Limits access to authorized users with Apono's JIT mechanisms.
<b>PR.AC-5 (Network Segmentation)</b>	Reduces access risks by limiting lateral movement through time-limited and context-based privileges.
<b>PR.AC-6 (Least Privilege Principle)</b>	JIT directly implements this principle by minimizing standing privileges.
<b>Detect Function</b>	
<b>DE.CM-7 (Monitoring Access and Privileges)</b>	Enables monitoring of temporary access activities to detect anomalies.
Requires timely disclosure of material changes in financial conditions or operations.	Limits access to financial systems to authorized personnel during critical reporting periods, reducing the likelihood of unauthorized changes that could lead to non-compliance or delays in disclosure.
 <b>NIST SP 800-63-3 (Digital Identity Guidelines)</b>	
<b>Identity Assurance Level (IAL), Authentication Assurance Level (AAL) and Federation Assurance Level (FAL)</b>	Apono's JIT access solution ensures that users are authenticated appropriately before access is granted, often meeting specific AAL requirements for sensitive tasks.
 <b>NIST SP 800-207 (Zero Trust Architecture)</b>	
<b>Dynamic Policy Enforcement</b>	Ensures that access is dynamically granted based on a combination of contextual factors (e.g., role, time, task).
<b>Continuous Authentication and Monitoring</b>	Eliminates risky standing privileges and enforces real-time validation of access needs.



## NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)

<b>3.1.5 (Least Privilege)</b>	Ensures users operate under the least privilege necessary to complete their tasks.
<b>3.1.7 (Prevent Non-Privileged Users from Executing Privileged Functions)</b>	JIT access restricts users from gaining access to sensitive systems or functions unless explicitly required.
<b>3.5.3 (Multi-Factor Authentication)</b>	Apono provides an additional layer of protection to require MFA, coupling with JIT access for heightened security.
<b>Link icon</b> <u>NIST SP 800-190 (Application Container Security Guide)</u>	
<b>Access Control Recommendations</b>	In containerized environments, JIT access ensures time-bound and need-based access for administrators and developers.

### 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. © 2025 Apono Inc; All rights reserved.

APONO

[www.apono.io](https://www.apono.io)  
 @Apono\_official  
 @aponoio