Compliance Mapping

NIST SP 800-53

How Admin By Request Helps

Document Information

Code: **MD-HAH-NIST-SP800-53**
Version: **1.0**
Date: **17 April 2025**

Admin By Request
ZERO TRUST PLATFORM

NIST SP 800-53 - How Admin By Request Helps

The following table outlines how Admin By Request helps your organization comply with the NIST SP 800-53 framework.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
AC-1 Policy and Procedures A. Develop, document, and disseminate: 1. Access control policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; B. Designate an official to manage the development, documentation, and dissemination of the access control policy and procedures; and C. Review and update the current access control: 1. Policy (organization-defined frequency and following organization-defined events); and 2. Procedures (organization-defined frequency and following organization-defined events).	Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy, or be represented by multiple policies reflecting the complex nature of organizations. Procedures: • can be established for security and privacy programs, for mission or business processes, and for systems, if needed. • describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. • can be documented in system security and privacy plans or in one or more separate documents.	Admin By Request aids in implementing robust *policies and procedures* by providing privileged access management capabilities. It allows organizations to enforce the **principle of least privilege**, ensuring that users only have elevated privileges when necessary. This aligns with SOC 2 criteria related to access controls and authorization.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.	
AC-2 Account Management A. Define and document the types of accounts allowed and specifically prohibited for use within the system; B. Assign account managers; C. Specify prerequisites and criteria] for group and role membership; 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) for each account; D. Require approvals by personnel or roles for requests to create accounts; E. Create, enable, modify, disable, and remove accounts in accordance with policy, procedures, prerequisites, and criteria; F. Monitor the use of accounts; G. Notify account managers and personnel or roles within: 1. time period when accounts are no longer required; 2. time period when users are terminated or transferred; and 3. time period when system usage or need-to-know changes for an individual; H. Authorize access to the system based on: 1. A valid access authorization;	Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts. Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts.	Admin By Request aids in implementing robust *account management* by providing privileged access management capabilities. It allows organizations to enforce the **principle of least privilege**, ensuring that users only have elevated privileges when necessary. This aligns with SOC 2 criteria related to access controls and authorization.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
2. Intended system usage; and 3. Other organization-defined attributes (as required); I. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; J. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and K. Align account management processes with personnel termination and transfer processes.	Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability.	
AC-2 (2) Account Management: Automated Temporary and Emergency Account Management Automatically remove and/or disable temporary and emergency accounts after a set time period for each type of account.	Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts, including local logon accounts used for special tasks or when network resources are unavailable (may also be known as accounts of last resort). Such accounts remain available and are not subject to automatic disabling or removal dates.	A feature of Admin By Request is its *Break Glass* capability, which allows administrators to create a new, temporary, one-time-use Administrator account that works on domains, Azure AD and stand-alone endpoints. This account audits all elevated activity while in use and terminates within a predefined amount of time or on log out. ***Break Glass* security elements** • Circumvents the need to use the built-in Windows local Administrator account – you can disable it completely to add an extra later of security to your endpoints. • The account must be used within an hour of being generated, minimizing the potential attack window and risk of account compromise. • One-time-only log in functionality: the user can log in once, and after log out, the account is terminated.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	Conditions for disabling or deactivating accounts include when shared/group, emergency, or temporary accounts are no longer required and when individuals are transferred or terminated. Changing shared/group authenticators when members leave the group is intended to ensure that former group members do not retain access to the shared or group account. Some types of system accounts may require specialized training. Management of temporary and emergency accounts includes the removal or disabling of such accounts automatically after a predefined time period rather than at the convenience of the system administrator. Automatic removal or disabling of accounts provides a more consistent implementation.	• The user has only the time specified under an Expiry setting when the Break Glass account was generated to use the administrator account; this duration is indicated on the built-in desktop background of each account. When the time-period is up, the session is terminated. • Measures are in place to ensure the Expiry time cannot be tampered with: if the Account user attempts to extend their time limit by adjusting the clock, the Account automatically logs out / terminates. • All user names and passwords are automatically generated, random, and complex, minimizing the possibility for a successful brute force attack. • Passwords are encrypted and stored within the web application, only accessible by Admin Portal users (i.e. IT Admins) via credentials – a safer option compared to MS LAPS' storage of admin account passwords in plain text along with the AD computer record.
AC-2 (6) Account Management: Dynamic Privilege Management Implement organization-defined dynamic privilege management capabilities.	In contrast to access control approaches that employ static accounts and predefined user privileges, dynamic access control approaches rely on run-time access control decisions facilitated by dynamic privilege management, such as attribute-based access control. While user identities remain relatively constant over time, user privileges typically change more frequently based on ongoing mission or business requirements and the operational needs of organizations.	Admin By Request addresses this requirement as it allows your organization to grant privileged access on a per application basis or in a restricted time window.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	An example of dynamic privilege management is the immediate revocation of privileges from users as opposed to requiring that users terminate and restart their sessions to reflect changes in privileges. Dynamic privilege management can also include mechanisms that change user privileges based on dynamic rules as opposed to editing specific user profiles. Examples include automatic adjustments of user privileges if they are operating out of their normal work times, if their job function or assignment changes, or if systems are under duress or in emergency situations. Dynamic privilege management includes the effects of privilege changes, for example, when there are changes to encryption keys used for communications.	
AC-2 (7) Account Management: Privileged User Accounts A. Establish and administer privileged user accounts in accordance with either a role-based access scheme or an attribute-based access scheme; B. Monitor privileged role or attribute assignments; C. Monitor changes to roles or attributes; and D. Revoke access when privileged role or attribute assignments are no longer appropriate.	Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration. A role-based access scheme organizes permitted system access and privileges into roles. In contrast, an attribute-based access scheme specifies allowed system access and privileges based on attributes.	You can set up different user groups with different sub-settings in Admin By Request to require approval for some, while not requiring approval for others. All activities can be audited in the auditlog.
AC-3 (2) Access Enforcement: Dual Authorization Enforce dual authorization for organization-defined privileged commands and/or other organization-defined actions.	Dual authorization, also known as two-person control, reduces risk related to insider threats. Dual authorization mechanisms require the approval of two authorized individuals to execute.	Through integrations, you can setup dual authorization work flows in, e.g. Jira, to ensure dual authorization.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	To reduce the risk of collusion, organizations consider rotating dual authorization duties. Organizations consider the risk associated with implementing dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.	
AC-3 (7) Access Enforcement: Role-based Access Control Enforce a role-based access control policy over defined subjects and objects and control access based upon organization-defined roles and users authorized to assume such roles.	Role-based access control (RBAC) is an access control policy that enforces access to objects and system functions based on the defined role (i.e., job function) of the subject. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on the systems associated with the organization-defined roles. When users are assigned to specific roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a large number of individuals) but are instead acquired through role assignments. RBAC can also increase privacy and security risk if individuals assigned to a role are given access to information beyond what they need to support organizational missions or business functions. RBAC can be implemented as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.	You can set up different user groups with different sub-settings in ABR to ensure that users with different roles have the access they need.
AC-5 Separation of Duties A. Identify and document organization-defined duties of individuals requiring separation; and	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.	By enabling "Require approval" in Admin By Request, another person will need to approve a user's privileged access before it is granted. In this way, duties are separated.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
B. Define system access authorizations to support separation of duties.	Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties.	
AC-6 Least Privilege Employ the **principle of least privilege**, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.	Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve least privilege. Organizations apply least privilege to the development, implementation, and operation of organizational systems.	By removing admin rights from all users and granting privileges on a per-application basis or for a limited time, you will be able to demonstrate enforcement of the **least privilege principle**.
AC-6 (1) Least Privilege: Authorized Access to Security Functions Authorize access for *authorized personnel* to carry out itemized *security functions*, with *security-relevant information*.	*Security functions* include establishing system accounts, configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. *Security-relevant information* includes filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, and access control lists.	By pre-approving applications and/or requesting a reason for elevation requests, you can ensure all elevated privileges are fully considered prior to granting access.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	Authorized personnel include named individuals or roles such as security administrators, system administrators, system security officers, system programmers, and other privileged users.	
AC-6 (2) Least Privilege: Non-privileged Access for Non-security Functions Require that users of system accounts (or roles) with access to itemized security functions and/or security-relevant information use *non-privileged accounts or roles*, when accessing non-security functions.	Requiring the use of *non-privileged accounts* when accessing non-security functions limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies, such as role-based access control, and where a change of role provides the same degree of assurance in the change of access authorizations for the user and the processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.	The setting *SSO Account Separation* requires the use of a different account for carrying out privileged operations. This option meets the requirements for Cyber Essentials Plus.
AC-6 (5) Least Privilege: Privileged Accounts Restrict privileged accounts on the system to organization-defined personnel or roles.	Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from accessing privileged information or privileged functions. Organizations may differentiate in the application of restricting privileged accounts between allowed privileges for local accounts and for domain accounts, provided that they retain the ability to control system configurations for key parameters and as otherwise necessary to sufficiently mitigate risk.	Privileged user logins can be grouped and assigned privileges for creating or updating any combination of the following: • user accounts • endpoint settings • inventory • approval requests • auditlog • reporting • remote access • support assist
AC-6 (6) Least Privilege: Privileged Access by Non-organizational Users Prohibit privileged access to the system by non-organizational users.	An organizational user is an employee or an individual considered by the organization to have the equivalent status of an employee.	In addition to full integration with an organization's single sign-on (SSO) implementation, *Vendor Access* is a remote access feature that allows specific, limited access via web portal to external parties.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.	All logins and operations carried out are fully audited.
AC-6 (7) Least Privilege: Review of User Privileges A. Review at a predetermined frequency the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and B. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.	The need for certain assigned user privileges may change over time to reflect changes in organizational mission and business functions, environments of operation, technologies, or threats. A periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be re-validated, organizations take appropriate corrective actions.	By removing admin rights, Admin By Request eliminates the need for review in most cases and facilitates the review of special cases (exclusions, Domain Admins, Break Glass accounts etc.) via a full audit trail and reporting.
AC-6 (8) Least Privilege: Privilege Levels for Code Execution Prevent the listed software from executing at higher privilege levels than the logged-in users executing the software.	In certain situations, software applications or programs need to execute with elevated privileges to perform required functions. However, depending on the software functionality and configuration, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications or programs, those users may indirectly be provided with greater privileges than assigned.	Since Admin By Request is a privileged access management solution, by definition, it focuses on minimizing the risks associated with granting administrative privileges to users. Any software that tries to execute with elevated privileges will be intercepted, asking for one of the following: • confirmation that it's OK to proceed • submission of a "Request for Approval", which must be granted by an authorized party • administrator credentials depending on settings specified in the Admin Portal.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
		Code Execution **security elements:** **Application Control Policies:** Admin By Request can enforce application control settings that restrict which applications can run on endpoints. By configuring these settings, including the ability to pre-approve "good apps" and block "bad apps", administrators can prevent unauthorized software from executing with elevated privileges. **Least Privilege Principle:** The solution adheres to the *principle of least privilege*, which means that users are only granted the permissions necessary to perform their tasks. This helps mitigate the risk of software running with unnecessary elevated privileges. **Privilege Elevation:** Admin By Request provides a controlled mechanism for elevating privileges on an as-needed basis. Instead of granting permanent administrative rights to users, it allows them to request elevated privileges for specific tasks, which are then subject to approval by administrators. **Auditing and Logging:** The solution includes auditing and logging capabilities to track software execution and privilege elevation activities. **Integration with Security Tools:** Admin By Request can integrate with other security tools and solutions, such as antivirus software and endpoint detection and response (EDR) systems. This integration enhances the overall security posture by providing additional layers of protection against malware and unauthorized software execution.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
AC-6 (9) Least Privilege: Log Use of Privileged Functions Log the execution of privileged functions.	The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to detect such misuse and, in doing so, help mitigate the risk from insider threats and the advanced persistent threat.	Admin By Request's auditlog provides full auditability with a tamper-proof record of privileged activities carried out by users.
AC-6 (10) Least Privilege: Prohibit Non-privileged Users from Executing Privileged Functions Prevent non-privileged users from executing privileged functions.	Privileged functions include disabling, circumventing, or altering implemented security or privacy controls, establishing system accounts, performing system integrity checks, and administering cryptographic key management activities. Privileged functions that require protection from non-privileged users include circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms. Non-privileged users are individuals who do not possess appropriate authorizations. Preventing non-privileged users from executing privileged functions is enforced by AC-3.	Admin rights are revoked from all users and you can configure Admin By Request to require approval for each elevation.
AC-17 Remote Access A. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and B. Authorize each type of remote access to the system prior to allowing such connections.	*Remote access* is access to organizational systems (or processes acting on behalf of users) that communicate through external networks such as the Internet. Types of remote access include dial-up, broadband, and wireless.	Admin By Request includes a feature called *Secure Remote Access* (also known as Remote Access):

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
	Organizations use encrypted virtual private networks (VPNs) to enhance confidentiality and integrity for remote connections. The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. VPNs with encrypted tunnels can also affect the ability to adequately monitor network communications traffic for malicious code. Remote access controls apply to systems other than public web servers or systems designed for public access. Authorization of each remote access type addresses authorization prior to allowing remote access without specifying the specific formats for such authorization. While organizations may use information exchange and system connection security agreements to manage remote access connections to other systems, such agreements are addressed as part of CA-3. Enforcing access restrictions for remote access is addressed via AC-3.	*Unattended Access* is a feature of Secure Remote Access that allows you to connect remotely to your servers and network endpoints directly from your browser, using a lot of the well-known Admin By Request features like: inventory, auditlog, settings and sub-settings, approval flows, integrations etc.The implementation of *Unattended Access* can use either a "Cloud" or an "On-premise" gateway, eliminating the need for VPN and jump servers, while still maintaining a secure and segregated setup. Using *Remote Access* does not restrict any of Admin By Request's functionality. In particular, the following apply: • Users requesting remote access are notified of their obligations and requirements (e.g. Code of Conduct) and must accept these before proceeding. • IT Admins can stipulate that emote sessions must be authorized before access is granted. Further, any elevated tasks a remote user might wish to run while remotely connected must be authorized separately, maintaining end-to-end security. ***Remote Access* security elements:** The elements described below illustrate how Admin By Request's *Secure Remote Access* product can assist with monitoring and control of remote access.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
AC-17 (1) Remote Access: Monitoring and Control Employ automated mechanisms to monitor and control remote access methods.	Monitoring and control of remote access methods allows organizations to detect attacks and help ensure compliance with remote access policies by auditing the connection activities of remote users on a variety of system components, including servers, notebook computers, workstations, smart phones, and tablets. Audit logging for remote access is enforced by AU-2. Audit events are defined in AU-2a.	**Session recording and auditing**: *Remote Access* includes the ability to record sessions for auditing and compliance purposes. This allows administrators to review activities performed during remote sessions and identify any unauthorized or suspicious behavior. **Session timeout and idle session management**: To mitigate the risk of unauthorized access in case of session abandonment or inactivity, *Remote Access* includes session timeout and idle session management features. These automatically terminate inactive sessions after a predefined period of time.
AC-17 (2) Remote Access: Protection of Confidentiality and Integrity Using Encryption Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.	**Encryption**: Data transmitted over the network is encrypted and remains confidential, ensuring it cannot be intercepted or tampered with by unauthorized parties.
AC-17 (3) Remote Access: Managed Access Control Points Route remote accesses through authorized and managed network access control points.	Organizations consider the Trusted Internet Connections (TIC) initiative DHS TIC requirements for external network connections, since limiting the number of access control points for remote access reduces attack surfaces.	**Role-based access control (RBAC)**: *Remote Access* participates in RBAC via Admin By Request's global settings and sub-settings, ensuring that only authorized users have access to specific features and functionalities based on their roles within the organization. This helps in limiting access to sensitive systems and data. **Access control sub-settings**: Administrators can define granular access control sub-settings to restrict the actions that remote users can perform on the target systems. This helps in enforcing security best practices and minimizing the risk of unauthorized changes or data breaches.

Control (ID, Name)	Control (Discussion)	How ABR helps with compliance
AC-17 (4) Remote Access: Privileged Commands and Access A. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for organization-defined needs; and B. Document the rationale for remote access in the security plan for the system.	Remote access to systems represents a significant potential vulnerability that can be exploited by adversaries. As such, restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and the susceptibility to threats by adversaries to the remote access capability.	**Multi-factor authentication (MFA)**: Implementing MFA adds an extra layer of security by requiring users to provide multiple forms of authentication before gaining access to the remote system.
AC-17 (6) Remote Access: Authenticate Remote Commands Implement appropriate organization-defined mechanisms to authenticate relevant organization-defined remote commands.	Authenticating remote commands protects against unauthorized commands and the replay of authorized commands. The ability to authenticate remote commands is important for remote systems for which loss, malfunction, misdirection, or exploitation would have immediate or serious consequences, such as injury, death, property damage, loss of high value assets, failure of mission or business functions, or compromise of classified or controlled unclassified information. Authentication mechanisms for remote commands ensure that systems accept and execute commands in the order intended, execute only authorized commands, and reject unauthorized commands. Cryptographic mechanisms can be used, for example, to authenticate remote commands.	**Integration with existing security infrastructure**: *Remote Access* is an integral part of Admin By Request, which integrates with existing security infrastructure such as firewalls, anti-virus software, and SIEM (Security Information and Event Management) systems to provide comprehensive protection against security threats. **Regular software updates and patches**: *Remote Access* is part of Admin By Request's Software Development Life Cycle (SDLC), meaning regular software updates and patches are applied. These are crucial for addressing security vulnerabilities and ensuring that the remote access solution remains resilient against emerging threats. Refer to Secure Remote Access for more information.

Document History

Version	Author	Changes
1.0 17 April 2025	Steve Dodson	Initial document release.