Compliance Mapping

ISO 27001

How Admin By Request Helps

Document Information

Code: **MD-HAH-ISO27001**
Version: **1.0**
Date: **17 April 2025**

Admin By Request
ZERO TRUST PLATFORM

ISO 27001 - How Admin By Request Helps

The following table outlines how Admin By Request helps your organization comply with the ISO 27001 framework.

ISO 27001 Control	Control Objective	How ABR helps with compliance
Requirements of the Information Management System		
9.1 Monitoring, measurement, analysis and evaluation		Admin By Request includes monitoring and auditing features that allow you to track and review elevation requests, system activities, and user behavior. This aligns with the ISO 27001 requirement for regular monitoring and analysis of user access to identify any unauthorized or inappropriate activities. Any evaluation effort for the part of your ISMS concerning privileged access will be easy and effective with the auditlog in the Admin By Request portal.
9.2 Internal audit		When performing internal audits, it is important that your auditor is able to review relevant information and export data. The auditlog in Admin By Request ensures full auditability with correct and tamper-proof records.
9.3 Management review		Auditlogs and traceability are essential to provide transparent and efficient reports to the management. This enables management and other stakeholders to take important decisions and evaluate the need for a more strict or loose approach towards management of privileged access. Admin By Request strengthens accountability by documenting and logging privileged access and reduces the risk of GDPR fines and litigation by ensuring transparency in privileged access logs.
10 Improvement		
Annex A Controls		
A.8.1.3 Acceptable use of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up.	An automated solution with secure work flows for elevating applications on the users' endpoints will remove the need for manual procedures, the effectiveness of which is dependent on the user's willingness to comply. When using Admin By Request, you will know that the user elevates applications only when they are allowed to do so.

ISO 27001 Control	Control Objective	How ABR helps with compliance
A.9.1.1 Access Control Policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Policies on management of privileged access are essential to any access control policy. To manage these with a tool such as Admin By Request will ensure positive feedback from your auditors.
A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Admin By Request is a Privileged Access Management solution. By definition, the answer to this control objective.
A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	As utility programmes can be downloaded from the internet, users must be restricted in their ability to install such software. Elevation of such programmes should be logged and monitored/reviewed periodically as well. All of this can be enforced using Admin By Request.
A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	The Admin By Request auditlog provides for a full record of all privileged access user activity including installs, uninstalls, elevated processes, duration, time, dates etc.
A12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	The Admin By Request auditlog can only be accessed in the Admin By Request portal by portal users. You can enforce access to the portal with SSO and MFA to further ensure only authorized access. Further, the auditlog cannot be changed or deleted and is therefore fully tamper-proof.
A.12.4.3	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	The auditlog provides information on all users with Admin By Request on their endpoint. Furthermore, the Settings Change log also provides information on which portal users have changed settings and when.
A.12.6.2	Rules governing the installation of software by users shall be established and implemented.	Admin By Requests enables your organization to restrict software installations in a proportional manner that fits into your risk assessments. The flexibility of the many different configuration options allows both a strict approach as well as a less strict approach - all while maintaining full productivity for your employees.
A.12.7.1	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	Access and review of auditlogs does not interfere with the usage of Admin By Request or disrupt any other service in the organization.

ISO 27001 Control	Control Objective	How ABR helps with compliance
A.14.2.1	Rules for the development of software and systems shall be established and applied to developments within the organization.	Your developers may fear that they need to request approval to elevate all applications. However, for certain groups of users, you can ensure auditlogs of their elevations by using *Admin Sessions* which allows them to act as admin for a limited period of time. In this way, you can add control to your SDLC while maintaining efficiency and seamless work procedures in your development team.
A.16.1.6 Learning from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Collection of evidence is crucial to be able to learn from and to recover from a security incident. A comprehensive log such as the Admin By Request auditlog will be useful to gather potential evidence.
A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	

Document History

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