Compliance Mapping

NIS 2

How Admin By Request Helps

Document Information

Code: **MD-HAH-NIS2**
Version: **1.0**
Date: **17 April 2025**

Admin By Request
ZERO TRUST PLATFORM

NIS2 - How Admin By Request Helps

The following table outlines how Admin By Request helps your organization comply with the NIS2 framework.

Paragraph	Objective	How ABR helps to ensure compliance
Paragraph 49	Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats. ENISA should monitor and analyze Member States' cyber hygiene policies.	Admin By Request can help your organization to securely manage software installs. It enables you to ensure that only authorized personnel are allowed to initiate and oversee new installs. This controlled access, complemented by monitoring features, provides an added safeguard, shielding the company's infrastructure from potential threats associated with the introduction of new software.
Paragraph 54	In recent years, the Union has faced an exponential increase in ransomware attacks, in which malware encrypts data and systems and demands a ransom payment for release. The increasing frequency and severity of ransomware attacks can be driven by several factors, such as different attack patterns, criminal business models around 'ransomware as a service' and cryptocurrencies, ransom demands, and the rise of supply chain attacks. Member States should develop a policy addressing the rise of ransomware attacks as part of their national cybersecurity strategy.	Admin By Request acts as guardian against ransomware by enforcing the principle of least privilege, ensuring users have *only* the necessary access for *only* the amount of time they need it. It also enables you to monitor and log privileged activities.

Paragraph	Objective	How ABR helps to ensure compliance
Paragraph 85	Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyber attacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.	Mitigating the risk of access to your resources by, e.g., an external consultant, you can utilize the Remote Access feature in Admin By Request Server Editions to mitigate the risk of remote access to your servers.
Paragraph 89	Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness. These entities should also schedule regular training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, the entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.	Entities can address this objective with Admin By Request by managing all privileged access within their organization. Further, machine learning capabilities for elevation approval can be enabled.

Paragraph	Objective	How ABR helps to ensure compliance
Paragraph 102	Where essential or important entities become aware of a significant incident, they should be required to submit an early warning without undue delay and in any event within 24 hours. That early warning should be followed by an incident notification. The entities concerned should submit an incident notification without undue delay and in any event within 72 hours of becoming aware of the significant incident, with the aim, in particular, of updating information submitted through the early warning and indicating an initial assessment of the significant incident, including its severity and impact, as well as indicators of compromise, where available. A final report should be submitted not later than one month after the incident notification. The early warning should include only the information necessary to make the CSIRT, or where applicable the competent authority, aware of the significant incident and allow the entity concerned to seek assistance, if required. Such early warning, where applicable, should indicate whether the significant incident is suspected of being caused by unlawful or malicious acts, and whether it is likely to have a cross-border impact. Member States should ensure that the obligation to submit that early warning, or the subsequent incident notification, does not divert the notifying entity's resources from activities related to incident handling that should be prioritized, in order to prevent incident reporting obligations from either diverting resources from significant incident response handling or otherwise compromising the entity's efforts in that respect. EN Official Journal of the European Union 27.12.2022 L 333/99: "In the event of an ongoing incident at the time of the submission of the final report, Member States should ensure that entities concerned provide a progress report at that time, and a final report within one month of their handling of the significant incident."	The Admin By Request auditlog makes it easy to audit and report on all activity undertaken by users while they have elevated privileges.

Document History

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