



Complying with the mandate T5.2.2: Privilege Management with ARCON | Privileged Access Management (PAM) solution

Table of Content

1. Cyber Ecosystem in the UAE (United Arab Emirates)
2. Purpose of the IT security standard in UAE
3. What exactly is NESA?
4. NESA Compliance is meant for whom?
5. What are the core objectives of NESA compliance?
6. Role of Privileged Access Management (PAM) in complying with NESA
7. NESA Compliance Checklist
8. Conclusion

Cyber Ecosystem in the UAE (United Arab Emirates)

The UAE (United Arab Emirates) dynamic economy has resulted in a very dynamic and the evolving digital ecosystem including expanding cybersecurity landscape since the last few years.

Towards this end, The National Cybersecurity Strategy (NCS) of UAE aims to create a safe and robust cyber infrastructure. It empowers citizens and businesses while protecting critical information assets in key industries. However, IT security challenges and risks surmount simultaneously with the introduction of innovative technologies or even improvisation in existing technologies.

Recently the UAE released Cybersecurity Report 2024 that highlights urgent cyber threats and defensive strategies. Released by the UAE Cyber Security Council and CPX Holding, this report says that more than 40% of critical vulnerabilities have been unaddressed for over five years. And Government, Energy, and IT sectors are the primary targets.

Purpose of the IT security standard in the UAE

The purpose of adhering to the IT security standards in the UAE is to raise the minimum level of protection for information assets and supporting systems across all entities from evolving cyber threats, including hacktivists and organized cybercrime groups. The objective is to –

- Risk-Based Approach: Entities follow a risk-based approach to implement information security assurance.
- Roles and Responsibilities: Clear delineation of roles for planning, development, implementation, and ongoing monitoring of IA.
- Sector-Specific Controls: Specialized controls tailored to sector-specific requirements.
- Incremental Adoption: Phased implementation to address common threats and optimize value.
- Compliance: Clarity on standard regulatory compliances of the region.

What exactly is NESA?

The National Electronic Security Authority (NESA) was formed in June 2014. It declared some key security policies to synchronize with the existing national cyber-security norms of the United Arab Emirates (UAE). It is a UAE federal authority that comes under the Supreme Council for National Security. It refers to the adherence of organizations to cybersecurity standards and guidelines set forth by the UAE's National Electronic Security Authority (NESA). It is mandatory for all UAE government entities and other entities identified as critical national services.

With the growing cyber security awareness in the UAE, NESA has taken collective responsibility for information technology, digital innovation, and data security. There has been a new set of security guidelines for most government entities and others which are identified as critical by NESA. Hence, compliance with NESA becomes mandatory for most of the business entities. NESA security compliance includes practices of Critical Information Infrastructure Protection Policy (CIIP) and the Information Assurance Standards (IAS). NESA comes under the federal authority of UAE. That is responsible for initiation, supervision, and monitoring of how UAE cyber security standards and policies are implemented.

NESA Compliance is meant for whom?

NESA regulatory compliance is compulsory for all UAE government and private entities such as banks, insurance companies, telecommunication operators and all other entities that deal with personal and confidential information. It is mandatory for every stakeholder to be directly/indirectly associated with the national information. NESA highly recommends following the guidelines so that they can also take active participation in strengthening the UAE's digital security level.

What are the core objectives of NESA compliance?

In the backdrop of rising number of cyber challenges and data breach incidents, enterprises in the UAE are fast adapting to information security tools. Large, medium, and small organizations from every industry are giving high importance in securing their IT infrastructure and thus looking for solutions that can –

- Protect enterprise data assets from malicious insiders or tainted third party users.
- Due to sophisticated threat patterns, there is a constant fear of compromising data, that includes personal customer data, enterprise data, statutory records, financial data, operational information, etc.
- Seamlessly assess organizations' compliance status and engage with relevant security practices to stay aligned with the standards. Thus, NESA regulatory compliance standards were introduced and implemented to get rid of any cyber threat.

Thus, NESA regulatory compliance standards were introduced and implemented to get rid of any cyber threat.

Role of Privileged Access Management (PAM) in complying with NESA



Privileged Access Management (PAM) plays a crucial role in complying with NESA requirements. Here is how it helps organizations meet NESA compliance:




- Detecting risky behavioral profiles in the IT ecosystem: PAM solutions monitor and analyze user behavior, identifying any unusual or risky activities related to privileged accounts. This helps prevent unauthorized access and potential security breaches.
- Monitoring, controlling, and validating every access to target systems: PAM tools provide granular control over privileged access. They ensure that only authorized users can access critical systems and resources. All access attempts are logged and audited.
- Keeping log details of every privileged activity: PAM maintains detailed logs of privileged actions, including who accessed what, when, and for what purpose. These logs are essential for compliance reporting and incident investigation.





This has necessitated to develop an effective privileged access management strategy. To prevent unauthorized access to information systems, password abuse/misuse, account takeover, insider and third-party threats, a robust privileged access management (PAM) practice is required. Briefly, PAM enhances security by securing privileged accounts, monitoring access, and maintaining audit trails, all of which contribute to NESA compliance.


NESA Compliance Checklist

In this paper, we have discussed NESA mandate **T5.2.2: Privilege Management** in the below table and how ARCON | Privileged Access Management (PAM) solution helps organizations of UAE to comply with the mandates.

T5.2.2 Privilege Management Applicability Statement and Description	Does ARCON PAM help to comply?	Which ARCON PAM feature addresses it?
<p>Control: The entity shall restrict and control the allocation and use of privileges</p>		<p>ARCON PAM helps organizations to restrict random allocation and usage of privileges and eliminates misuse of elevated access rights with privileged user authorization and enforces fine-grained controls that includes Role-based-Access Control (RBAC) and Policy-Based Access Control (PBAC). Furthermore, ARCON auto-onboarding functionality on-boards all the privileged identities underlying in IT systems and scans infrastructure at regular intervals to ensure that there is no “orphaned” or “dormant” privileged identity that can be misused.</p>
<p>Sub Control:</p> <ol style="list-style-type: none"> 1) Maintain a record of all allocated privileges 2) Never grant users with domain or local administrative privileges 3) Ensure that administrator accounts are used only for system administration activities (e.g., no email or web surfing) 4) Use two-factor authentication for all administrative access 5) Ensure that all administrative access is logged and audited 		<ol style="list-style-type: none"> 1) ARCON PAM’s Audit Trails manages the lifecycle of privileged accounts as every activity performed by privileged users is captured in both video and text format. The record of reports in the form of video/ text includes detailed analytics of every allocated privilege that target critical systems and applications. 2) PEDM (Privilege Elevation and Delegation Management) of Endpoint Privilege Management (EPM) solution enables IT administrators to grant temporary elevated privileges to end users that need to perform specific project-based tasks on Windows, MacOS, Linux and Unix environments by following the principle of “Least Privileges.” 3) RBAC (Role-based Access Control) mechanism of ARCON PAM enforces necessary and relevant restrictions in the access control policies where any privileged account is entitled to get access to the only system/ application assigned for.

		<p>4) Multi-factor Authentication (MFA) of ARCON PAM ensures every privileged access is verified, authorized, and authenticated before allowing access to the critical systems.</p> <p>5) Same as point no. 1 (Audit Trails) above</p>
<p>Implementation guidance : Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process in accordance with the relevant access control policy</p>		<p>ARCON PAM offers MFA (Multi-factor authentication) that ensures every privileged access is verified, authorized, and authenticated before allowing access to the critical systems. This authorization of users ensures the implementation of an access control framework around people and policies.</p> <p>Moreover, a robust access control policy (endpoint controls) streamlines the complete process of identity protection setting up access perimeter. Furthermore, as the privileges in the solution are user centric (controlled through workflows), there is a layer for authorization of privileges too.</p>
<p>Implementation guidance : A. Identify privileged access rights associated with each system, e.g., operating system, database, and application</p>		<p>Access control of ARCON PAM enables organizations to define and enforce precise access policies for privileged users at granular level, reducing the risk of unauthorized access and misuse of sensitive enterprise data.</p>
<p>Implementation guidance : B. Privileged access rights should: - I) Be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy, i.e., the minimum requirement for their functional role only when needed II) Not be granted until the authorization process is completed III) Be assigned a different User ID than the User ID used for day-to-day work. Regular user activities should not be performed from privileged accounts</p>		<p>ARCON PAM helps organizations to control over-privileged access and ensure that this access is granted on a “need-to-know” and “need-to-do” basis. As a result, unnecessary access or unauthorized access is prevented seamlessly.</p> <p>The solution’s robust authorization and user authentication capabilities ensure that only valid authorized users are allowed access to the critical systems/ applications.</p> <p>ARCON PAM also offers PEDM (Privileged Elevation and Delegation Management) feature that allows authorized users to temporarily elevate their privileges to perform a specific task that requires higher privileges. Without compromising security, it provides a secure mechanism for granting privileged accounts’ temporary elevated access without exposing sensitive credentials to unauthorized users.</p>

		Moreover, Just-In-Time (JIT) privileges of ARCON PAM ensure time-based allocation of privileged access and automated revocation of privileged rights immediately after the completion of the assigned task(s). Hence, who to allow access for what, when and why does not require manual intervention.
<p>Implementation guidance :</p> <p>C. An authorization process and a record of all privileges allocated should be maintained</p>		One Admin Control of ARCON PAM provides a centralized control point that authorizes every access to the target systems. It enforces the implementation of an access control framework around people and policies only on a “need-to-know” and “need-to-do” basis.
<p>Implementation guidance :</p> <p>D. Requirements for expiry of privileged access rights should be defined</p>		Just-In-Time (JIT) privileges of ARCON PAM is a robust security mechanism that helps organizations with time-based allocation of privileged access and automated revocation of privileged rights immediately after the completion of the assigned task(s).
<p>Implementation guidance :</p> <p>E. The competences of users with privileged access rights should be reviewed regularly to verify if they are in line with their duties</p>		<p>ARCON PAM’s customized reporting engine helps enterprises to remain audit-ready by providing customized and detailed analytics and reports of every privileged access to target systems and their daily activities. This automatically verifies the privileged users’ activities and detects anomalies (if any).</p> <p>Moreover, the solution’s robust Identity Governing engine ensures that the right people have the right level of access to the right resources at the right time while mitigating risks. Governance of identity includes the entire lifecycle management of identities and asset governance.</p>
<p>Implementation guidance :</p> <p>F. Specific procedures should be established and maintained to avoid the use of generic administration User IDs, according to systems configuration capabilities</p>		ARCON PAM recommends avoiding the usage of generic administration user IDs for application use, by enforcing granular controls for endpoint accesses (setting up perimeter for endpoint access and layer of MFA). Furthermore, ARCON PAM maintains detailed audit trails for every action performed by the user/ administrator on the ARCON PAM application.

<p>Implementation guidance :</p> <p>G. For generic administration User IDs, the confidentiality of security credentials should be maintained when shared (changing them frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms)</p>		<p>The Credential Vault engine of ARCON PAM enables organizations to generate complex, randomized passwords for privileged accounts that cannot be easily guessed or cracked. It allows organizations to enforce password policies such as password expiration and extent of complexity and rules to ensure that passwords are updated regularly and meet the organization's security standards. It eliminates the need for privileged users to remember and share passwords, thus lowering the risk of password misuse. It helps enterprises to secure credentials by employing strong encryption algorithms, including FIPS-approved Advanced Encryption Standard (AES) 256-bit encryption. This protects all the credentials stored in the vault from unauthorized access and ensures compliance with FIPS guidelines.</p>
--	---	---

Conclusion

ARCON | Privileged Access Management enables SRM leaders to:

- Comply with NESA guidelines pertaining to Privileged Identity Management
- Ensure robust privileged identity management environment enterprise-wide
- Mitigate the chances of data breach incidents and IT security vulnerabilities
- Meet the demands of advanced PAM use cases as highlighted in NESA compliance guidelines

about ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us    

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.