Predict | Protect | Prevent

NESA Compliance enhances resilience of UAE ICT Infrastructure

arcon

Introduction

Formed in June 2014, the National Electronic Security Authority (NESA) declared some key security policies to sync with the existing national cyber-security norms of the United Arab Emirates (UAE). It is basically a UAE federal authority that comes under the Supreme Council for National Security.

With the growing cyber security awareness in the UAE, NESA has taken collective responsibility of 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 to 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.

With an objective to protect UAE's enterprise IT environment, NESA contributes to the collective achievement of national goals. In this regard, His Excellency Jassem Bu Ataba Al Zaabi, Director General added,

> "Cyber security is one of the biggest economic and national security challenges countries face in the twenty-first century. The National Electronic Security Authority was established in line with this modern reality and as soon as the Authority was in place, we immediately initiated a thorough review of federal efforts to defend and protect the nation's ICT infrastructure. This announcement falls in line with the process we are currently engaged in which puts all necessary policies and standards in place to ensure a comprehensive approach to securing the nation's digital infrastructure."

> "NESA is committed to ensuring that all UAE government bodies are made fully aware of the responsibility they now have to meet the requirements of these policies and in turn, what this means in practice going forward," he also added.

(*Source: Press Release on NESA 'Cyber Security Program' in Abu Dhabi*)

Why NESA regulatory compliance was formed?

NESA regulatory compliance standards for UAE were formed with the following objectives:

Strengthen the security of the UAE's information assets and reduce risks

Secure crucial digital infrastructure (critical IT systems from cyber vulnerabilities)
Secure crucial digital infrastructure (critical IT systems from cyber vulnerabilities)

Increase awareness of cyber security threats in the country

Improve enterprise's IT security responsiveness and preparedness capabilities

Who should comply with NESA and why?

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 private information. It is mandatory for each and every stakeholder who is directly/ indirectly associated with the national information. NESA highly recommends to follow the guidelines so that they can also take active participation in strengthening the UAE's digital security level.

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 their data assets from malicious insiders or tainted third party users. Information security threats are not only rising but also getting sophisticated day by day and there is a constant fear of compromising data, which includes personal customer data, enterprise data, statutory records, financial data, operational information and the list goes on. Thus, NESA regulatory compliance standards were introduced and implemented to get rid of any cyber threat.

Compliance Mapping with ARCON

ISO/ IEC 27005:2005 Act

Objective

The ISO/ IEC 27005:2005 act (Information Security Risk Management act) mandates organizations to control information security and assess risks lying in the network infrastructure.

In a typical scenario where confidential information of an organization is accessed by multiple users including insiders, partners or even third parties, it generates risks related to data breach of those crucial data.

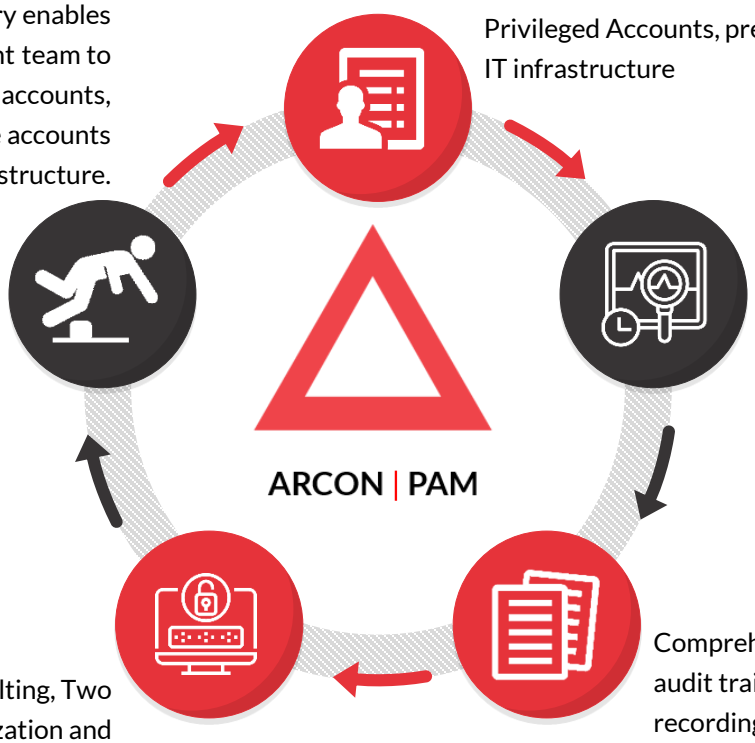
If there is no mechanism that can monitor the users about their activities, then it raises the risk of data breach related incidents. The accounts which gives access to sensitive information are privileged accounts and in most cases, risks surface from these privileged accounts if they are unmonitored and uncontrolled.

As a result, it becomes easy for the malicious actors to infiltrate and steal information from these privileged accounts for money. Hence, securing those privileged accounts is highly crucial to prevent data loss. Organizations having multiple privileged accounts in their network, have risks of being compromised by malicious insiders or third party users any time. In a shared and distributed environment, this risk increases and Privileged Access Management (PAM) helps in mitigating the risk of information breach. ARCON | PAM helps organizations to manage and control information security risks around privileged accounts.

How ARCON Privileged Access Management (PAM) helps in meeting compliance requirements while safeguarding your enterprise's critical information?

ARCON auto-discovery enables the risks management team to discover shared accounts, software and service accounts across the IT infrastructure.

ARCON enterprise-class PAM seamlessly tracks and monitors every single access to Privileged Accounts, present at any layer of IT infrastructure



Isolates anomalies in real time thereby preventing activities that could be fraudulent

Comprehensive reporting, audit trails and session recordings to ensure all privileged sessions are tracked

Secure password vaulting, Two Factor Authorization and database encryption among many other features ensure that your confidential information is secure from unauthorized access

ISO/ IEC 27032:2712 Act

Objective

This Information Security Guideline mandates implementation all the basic cyber security standards. It requires organization to build a security posture for responding to attacks. The act demands detecting and monitoring attacks in real-time.

How ARCON can reinforce your information security framework?

ARCON with it's enterprise class solutions such as Privileged Access Management (PAM), User Behaviour Analytics (UBA) and Security Compliance Management (SCM) offers a robust mechanism which allows to seamlessly manage and monitor IT users.

- ARCON | PAM is a highly effective solution which manages, controls and monitors privileged user activities within a centralized policy framework in an enterprise.
- ARCON | UBA is a self-learning user behaviour analytics tool that monitors each and every user to figure out suspicious activities and trigger alerts to the administrators in real time.
- ARCON | SCM is an automated vulnerability assessment tool that helps an organization to conduct real time assessment of the extent of security in all critical platforms and ensures the desired compliance level.

NIST 800-53 Revision 4 Act

Objective

This act mandates implementing best practices to safeguard privileged access.

How ARCON | PAM can provide you enterprise robust access control?

One Admin Control

ARCON | PAM provides a unified policy engine to offer a rule and role-based restricted privileged access to target systems. No matter how big the organization network is, every access to the critical systems is managed by One Admin Control.

Privileged Elevation and Delegation Management

This tool enables to elevate and delegate privilege tasks to non-admin users that require temporary access to target systems. After the privilege tasks are completed, access rights are revoked. The tool essentially helps in implementing the principle of least privilege.

Single-Sign-On (SSO)

Single-Sign-On provides one time administrative access to target systems. With this, the non-administrative users are prevented from accessing/ sharing information from the privileged accounts.

M5.5.4 (Security Control) Act

Objective

This Security Compliance Act says that organizations' IT security arrangements are able to meet with the other global regulatory standards such as EU GDPR, PCI DSS, SWIFT CSF, HIPAA.

For more information about how ARCON can meet the global regulatory standards, please visit the below link and download GDPR Compliance brochure, HIPAA Compliance brochure, PCI DSS Compliance brochure, SWIFT Compliance brochure.

How ARCON can provide granular level security?

ARCON | PAM offers deepest level of granular control by segregating privileged users in -

Granular control:

restricts and elevates privileged user commands for databases to control critical activities on target devices

Virtual Grouping:

enables the security team to segregate privileged users and their access to authorized database and applications based on assigned roles and duties

T5.5.4 (Security Control) Act

Objective

This Access Control Act says that enterprise privileged access control system should have the required security policies for access and segregation of user accounts.

T6.5.4 (Security Control) Act

Objective

This act mandates robust authentication mechanism.

ARCON | PAM offers a robust authentication mechanism.

ARCON | PAM offers deepest level of granular control by segregating privileged users in -

Multi-factor Authentication

- Multi-factor authentication (MFA) provides a robust validation mechanism by acting as a strategic entry point to identity management systems and help managing system based users.
- ARCON offers native software based One-Time-Password (OTP) validation to begin a privileged session and the tool seamlessly integrates with disparate third-party biometric authentication solutions such as Gemalto, RSA, Vasco, 3M, Precision, SafeNet and Safran.

Password Vault

- ARCON Password Vault is a robust engine that allows the enterprise IT security team to frequently randomize and change passwords.
- The electronic vault, which stores privileged passwords in a highly secure manner uses AES-256 bit encryption.
- It is further wrapped with a proprietary encryption algorithm.
- The electronic vault has release request workflow including secured printing to support emergency password retrieval in breakglass scenarios.

Conclusion

Misuse of corporate confidential information often stems due to inadequate identity & access control management. Privileged accounts, super admin accounts, that provide access to critical information are often operated with shared credentials and without proper mechanism in place to monitor and audit activities around 'trusted privileges'. Malicious insider/s or external malefactors could harm an enterprise by compromising information assets.

Managing and ensuring secure privileged access remains one of the biggest pain points for any organization. This enormous challenge arises due to high level of complexity involved in managing a large number of privileged accounts. If any of those trusted privileges are compromised, an enterprise could lose not only highly confidential information, but productivity would also take a hit due to regulatory implications.

Solution: Privileged Access Management. It provides a security blanket that sits on top of the entire IT infrastructure such as Operating systems, Databases, Network devices and Security devices. All Administrators, IT Operators and other privilege users including (Application Interfaces) are allowed to login to their authorized systems only by using a unique user ID, Password and OTP provided to them. Once logged in, view/modify access is provided only on "need to know" and " need to do" basis. Further, activities carried out are recorded and complete audit trails are maintained.

The bottom line: As vital information is stored in a distributed environment, enterprises today has one additional responsibility to safeguard information assets. It is imperative that a robust compliance and governance policies can be formulated by deploying automated tool such as Privileged Access Management, an enterprise not only gains operational efficiency, but also becomes adequately fortified to mitigate data breach risks.

arcon

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