NOVEMBER 1, 2022

NESA – STEP INTO INFORMATION SECURITY IN UAE

WHITE PAPER BY AUUDITR

Introduction

Information security is the mantra of the new world order where data and information are so much available yet vulnerable that security protocols and standards are now a necessity. The Signals Intelligence Agency, formerly known as National Electronic Security Authority, is the UAE intelligence agency that developed standards for guidance on information security. NESA is the UAE law that governmental, semi-governmental, and business-critical to the infrastructure must follow.

The standard has 188 controls as requirements to fulfill to achieve compliance. NESA guidelines are both technical and managerial. We shall further discuss the contents of this standard and Auuditr’s services to help companies achieve compliance.

> “NESA is the UAE law which governmental, semi-governmental and businesses critical to infrastructure must follow. "

Keywords: UAE NESA, Information Security, Security Controls, Auuditr, Cyber Security, Data Encryption, Risk Management

Context and structure

> “The strategy behind the development of this law is to be prepared for the unwanted scenarios and prevent them before occurring. “

The primary objective of this law is to provide information security leads on a national level. This law also promotes awareness related to cybersecurity and protects its citizens from data breaches and risks. The strategy behind the development of this law is to be prepared for unwanted scenarios and prevent them before occurring.

The standard consists of 188 security control divided into two streams

1. **Management Controls** – These controls are part of management processes and operations. These are further divided into six controls.
    a. **M1**: Strategy and Planning, which defines the management system as implementable processes.
    b. **M2**: Information Security Risk Management is to prevent any unwanted scenario from occurring.
    c. **M3:** Awareness and Training deal with the constant reminder to all the organization's entities about information security.
    d. **M4:** Human Resource Security, tackles the security measures while the intake of employees and after they leave.
    e. **M5:** Compliance checks the current state of the processes.
    f. **M6:** Performance Evaluation and Improvement deals with the overall information security rating in the organization and improves the system for better management.

2. **Technical Controls** – These deal with the technical aspects of information security, sometimes following the decisions from the management controls.
    a. **T1**: Asset Management deals with from purchasing of the asset to the disposal, keeping the information security intact.
    b. **T2**: Physical and Environmental Security describes the type of controls enforced to restrict the information.
    c. **T3**: Operations Management, which deals with the flow of processes within the information security ecosystem.
    d. **T4**: Communication talks about the measures that must be taken to keep information secure in all types of communications.
    e. **T5**: Access Control restricts the access of the irrelevant parties to the information and creates levels of access for organized management.
    f. **T6**: Third-Party Security deals with the vendors and suppliers that work with the organization for the operations upkeep.

g. **T7**: Information System Acquisition, Development, and Maintenance talks about the internal secure development processes and keeping the data protection policies intact while developing and maintaining activities.

h. **T8**: Information Security Incident Management guides the users about an organized way of tackling incidents and problem management.

i. **T9**: Information Security Continuity Management helps to understand the continuity of services during downtime while keeping the information security principles in mind.

These controls are further divided into implementable sections. Also, these controls are further tagged on priority levels P1 – P4 according to their impact.

The basic principles of the standard are like other cybersecurity laws and standards. The understanding behind information security is the same globally. Each region accepting these principles as laws shows the importance of data security and protection these days. By adopting these principles, governments are taking additional steps to protect their citizens and improve their national security.

> "By adapting these principles, governments are taking additional steps to protect their citizens and improving their national security."

Services Offered by Auuditr

As a consultancy firm, we offer our team the expertise to develop processes and management methods to ensure information security in organizations. We provide the following services:

- Gap assessment sessions to find out the existing capability of the organization
- Consultancy sessions
- Policies and procedure guidelines
- Tools and templates
- NESA compliance evaluation and final report

Auuditr works with the validation tools offered by the standard and helps the clients to assess and follow the set of requirements. We also provide consultancy sessions for the further management of information security within the organization.

Further information on

www.Auuditr.com