**Cybersecurity Framework**

Cybersecurity frameworks are instruction or guidance outlined for an organisation must follow to mitigate cybersecurity risks. Cybersecurity framework lays the requirement that an organisation adhere to in order to protect their system from malicious attacks. These frameworks are standard and can be followed by multiple organisations (Taherdoost, 2022). Information security standard and Information security Governance are 2 main cybersecurity standards. Networking infrastructure, Hardwares, software and users and information systems are important pasts of security standards.

There are multiple cybersecurity standards and framework available to cater to different needs of an organisation. Most commonly used cybersecurity standards are ISO 27000 series, ISF, SOFP, NIST, SOX and RISK IT(Taherdoost, 2022). It Highly crucial for an organisation to understand what each on is based on and select a standard that fits the best for them. However, some organisation will have to select more than on standard in case the needs are not met in one standard.

After doing considerable amount of research we have decided to select NIST framework. Stated below are some information about it and table describing its integration with azure (Taherdoost, 2022):

**Nations Institute Of Standard and Technology Cybersecurity (NIST) Framework**

In order for a company to rate its maturity NIST provides 3 main components; Core, Implementation tier and Profile (Alshar’e, 2023).

**Core**: The five-essential element of core process that helps in addressing security concerns are Identification, protection, reaction and recovery.

**Implementation Tier**: NIST have a maturity rating scale of 0 to 4 where zero being the lowest and 4 being the highest. These scores are used by the companies to establish a benchmark.

**Profile**: Regularly evaluating security risks and finding maturity level is very important for an organisation. It helps them prepare for the potential security risks that may rise. It also help them determine the priority that they should give to each task in order to mitigate the risk.

**Strengths of NIST Framework**

**Flexibility:**

* NIST can be tailored to adapt to organisation of different size and sector in order to implement customised needs and risk profile (Alshar’e, 2023).

**Comprehensive Approach:**

* NIST Framework covers wide variety if task including identification, protecting, detecting, responding and recovering from security incidents (Alshar’e, 2023).

**Best Practices and Guidelines:**

* The framework offers a strong foundation of best practices that businesses may use because it is built on top of currently in place standards and guidelines (Alshar’e, 2023).

**Risk Management Focus**:

* It focuses on risk based strategy to assist companies prioritising their cybersecurity activities according to the specific risk they face (Alshar’e, 2023).

**Enhanced Communication:**

* Promotes improved cybersecurity risk and assessment communication between stakeholders, management and technical team (Alshar’e, 2023).

**Encourages Continuous Improvement:**

* It helps organisation stay head of new potential threats by promoting a culture of ongoing assessment and enhancement of cybersecurity posture (Alshar’e, 2023).

**Weaknesses of NIST Framework**

**Implementation Challenges**:

* Companies, particularly those with little experience in cybersecurity, may find it challenging to understand and use the framework (Alshar’e, 2023).

**Resource-intensive:**

* Smaller firms with tighter budgets may find it difficult to implement the framework as it can take a lot of time and money (Alshar’e, 2023).

**Absence of precise measurements**:

* Organizations may find it challenging to statistically evaluate the success of cybersecurity programs due to the framework's lack of precise measurements (Alshar’e, 2023).

**Overemphasis on Compliance**:

* The framework's efficacy may be limited if certain firms utilize it exclusively for compliance requirements rather than as a proactive cybersecurity approach (Alshar’e, 2023).

**Dynamic Threat Landscape**:

* Organizations may find it difficult to keep up with the most recent risks and mitigation techniques as a result of the cyber threats' potential to evolve faster than the framework's upgrades (Alshar’e, 2023).

|  |  |  |
| --- | --- | --- |
| **NIST Function** | **Azure Service** | **Description** |
| Identify | Azure Security Centre | Offers consistent threat prevention and security management for hybrid cloud workloads. |
| Protect | Azure Policy | Assist in the mass evaluation of compliance and the enforcement of corporate standards. |
| Azure Active Directory | Offers services for managing access and identification. |
| Detect | Azure Firewall | Provides identity and access management, encryption, and network protection. |
| Azure Sentinel | Intelligent security analytics using cloud-native SIEM and SOAR solutions. |
| Respond | Azure Monitor | All-inclusive solution for gathering, examining, and responding to data from on-premises and cloud settings. |
| Azure Security Centre | Offers advanced threat protection and provides security alerts and incidents. |
| Recover | Azure Backup | Safeguards your apps and data, making sure you can restore them in the event of loss. |
| Azure Site Recovery | Helps maintain company continuity by keeping business apps and workloads operating during disruptions. |

**REFERENCE**

1. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, [online] 11(14), p.2181. doi:https://doi.org/10.3390/electronics11142181.
2. Alshar’e, M. (2023). CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. *Applied computing Journal*, 3(1), pp.245–255. doi:https://doi.org/10.52098/acj.202364.